CARESTREAM Vue PACS and Vue Archive 12.1 Administration Guide

Part 9J8767
2015-12-07

Table of Contents

Preface

CARESTREAM Vue PACS and Vue Archive

Trademark and Copyright Information

CARESTREAM is a trademark of Carestream Health.

This document is copyrighted with all rights reserved.

APPLE, IPAD and IPHONE are registered trademarks of Apple Inc.

SAMSUNG, GALAXY S and GALAXY NOTE are registered trademarks of Samsung Electronics Co.

Under the copyright laws, this document may not be copied, in whole or in part, without the written consent of Carestream Health, Inc. Under the law, copying includes translating into another language or format.

All names or identities used in this document are fictitious.

Caution: Federal law restricts this device to sale to, by, or on order of a physician.

The information contained herein is based on the experience and knowledge relating to the subject matter gained by Carestream Health, Inc. prior to publication. No patent license is granted by this information.

Carestream Health, Inc. reserves the right to change this information without notice and makes no warranty, express or implied, with respect to this information.

Carestream Health, Inc. shall not be liable for any loss or damage, including consequential or special damages, resulting from the use of this information, even if loss or damage is caused by Carestream Health, Inc.'s negligence or other fault.

Authorized Representative (European Union)

EC REP

Carestream Health France
1, rue Galilée
93192 NOISY-LE-GRAND CEDEX
FRANCE

CE 0086

Importer for European Union

Carestream Health Netherlands B.V.

Bramenberg 12

3755 BZ Eemnes

The Netherlands

1 Introduction

This document describes system administration tasks for CARESTREAM Vue PACS and Vue Archive. The administration tasks include:

- Managing users and groups
- Performing system configuration
- Performing system checks
- Performing database and configuration management
- Performing system administration tasks

1.1 Who Should Use This Document

This document is intended for use by system administrators who configure and update Vue PACS and Vue Archive at client sites.

2 Getting Started

2.1 Logging in to the CARESTREAM Vue Administration Tool

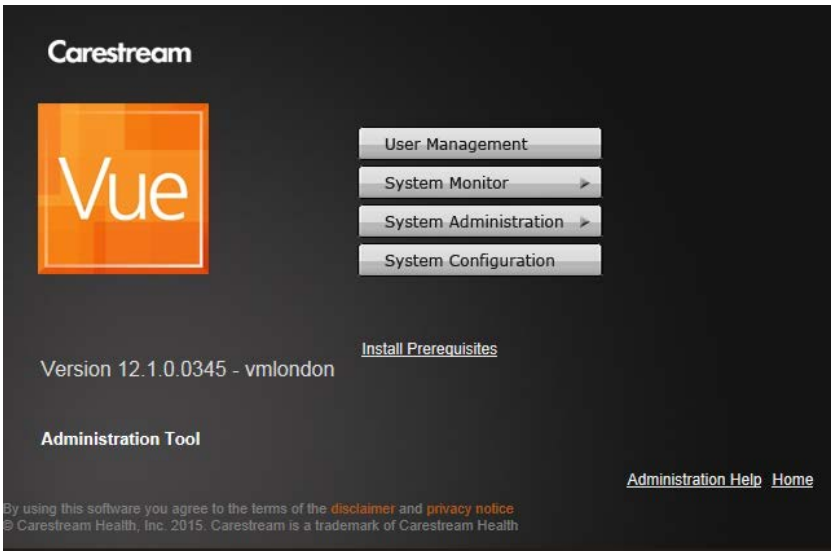
The CARESTREAM Vue Administration Tool is the gateway to the user management, system monitoring, system administration, and system configuration applications.

1. In your browser, type the address of the server and press **Enter**.

2. In the window that appears, click **Administration**.

   The **Administration Tool** menu appears. From here, you can access the user management, system monitoring, system administration, and system configuration applications.

   The log in procedure is the same for all applications. In this example, the log in to the User Management tool is described.



3. Click **User Management**. The **Login** window appears.

Note: When you log in for the first time, you are prompted to change your password.

4. In the **User** box, type your assigned login name.
5. In the **Password** box, type your password.
6. Click **OK** to log in.

3 Managing Users and Groups

If you are an authorized administrator, you can use the User Management Admin tool to define logical groups of users and define basic group and user details, such as central login criteria. You can also edit the default system settings (if you have permission to do so) to change the settings for all groups and users.

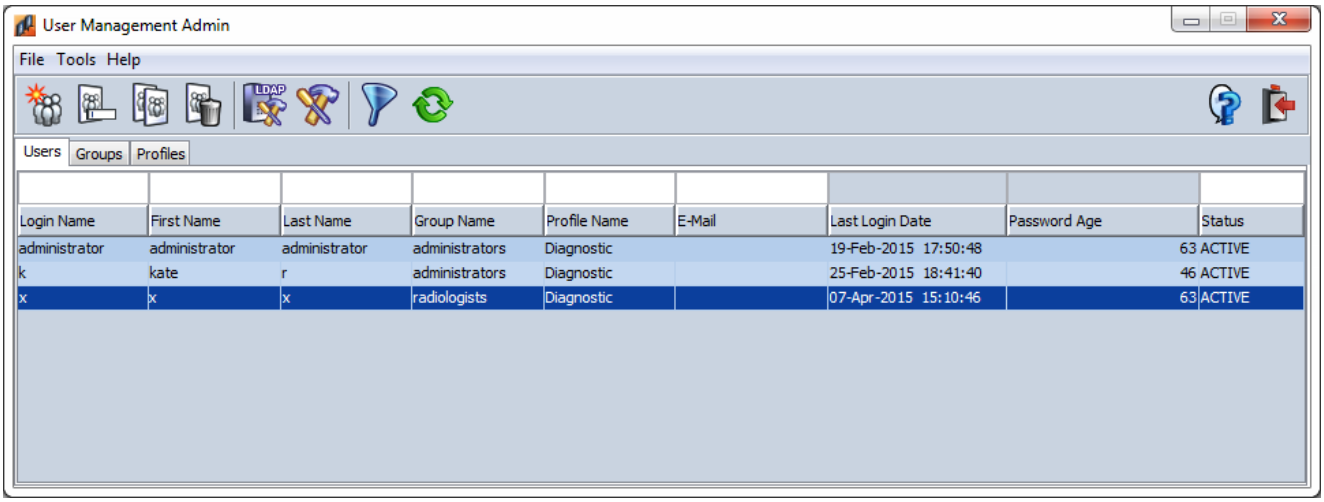
Note: During installation, one default administrator user is defined to start using the system with the default settings. Except for the default administrator, account users and groups initially have no privileges. The system administrator must set these before the system can be used.

You can use the User Management Admin tool for the following activities:

- Adding New Users and Groups
- Defining Advanced Settings for Users
- Defining External Applications for Users
- Editing Settings at the System, Group, and User Levels
- Deleting Users and Groups
- Assigning Restrictions to Users and Groups
- Modifying Permissions

3.1 Getting Started with the User Management Admin Tool

To open the User Management Admin tool, select **User Management** from the Administration Tool menu.



See Section 3.1.2 User Management Admin Tool Tabs for more information about the elements in each of the tabs in the User Management Admin tool.

Note: The **User Management Admin** window appears differently depending on whether your system is using a central MICROSOFT Active Directory server as the user repository (LDAP repository). When using an LDAP repository, only the **Groups** tab appears initially, as the user management is performed outside of the User Management Admin tool. See Section 3.1.3 Configuring the User Management Repository for more information.

3.1.1 Using the User Management Admin Toolbar

#	Description
1	**Import**—For LDAP configurations only—Click to import users from the LDAP repository
2	**Add New**—Click to add a new user or group
3	**Edit selected**—Click to edit the selected user or group
4	**Copy selected**—Click to copy the selected user or group
5	**Delete Selected**—Click to delete the selected user or group
6	**LDAP Settings**—Click to configure the user management repository
7	**System Settings**—Click to modify the system settings
8	**Filter**—Click to filter the results shown
9	**Refresh**—Click to refresh the display with the latest information
10	**Help**—Click to open the **About** window with copyright information
11	**Exit**—Click to close the application

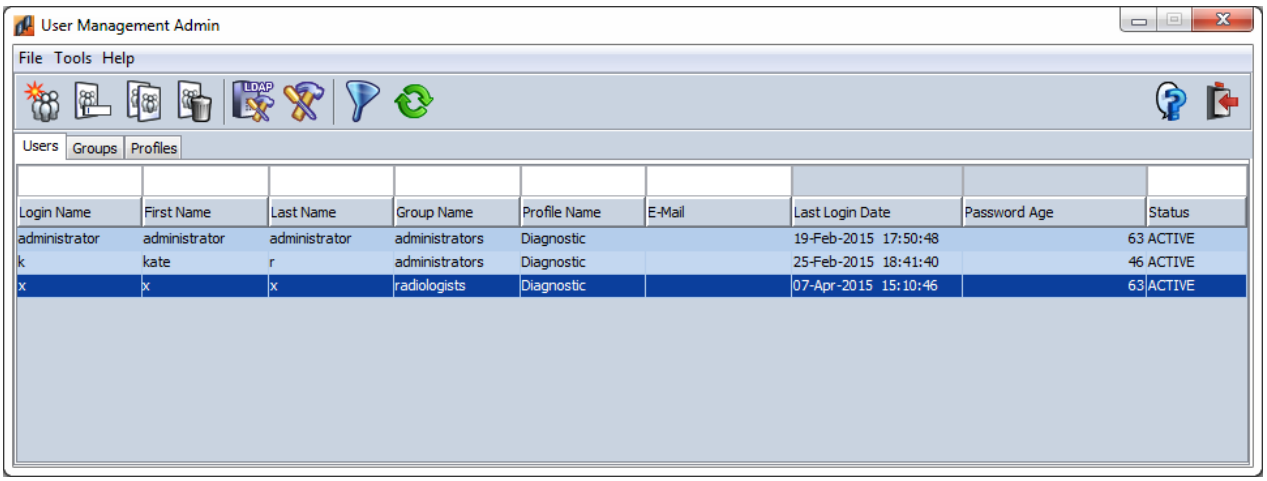
The User Management Admin toolbar is page-sensitive; when toolbar functions are not relevant to a particular page, they are grayed out.

3.1.2 User Management Admin Tool Tabs

The User Management Admin tool includes a **Users** tab, a **Groups** tab, and a **Profiles** tab.

3.1.2.1 Users Tab

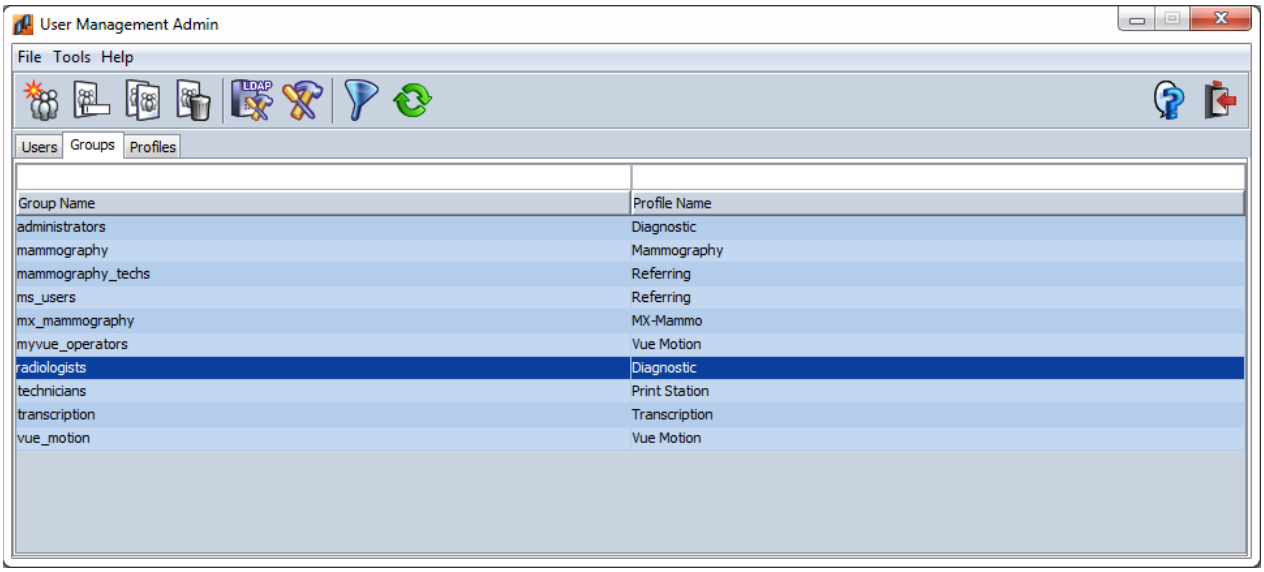
In the **Users** tab you can add, edit, and delete users and define user settings.



Element	Type	Description
Login Name	Column	The user's assigned login name.
First Name	Column	The user's first name.
Last Name	Column	The user's last name.
Group Name	Column	The group to which the user is assigned by the administrator.
E-Mail	Column	The user's email address.
Last Login Date	Column	The date on which the user last logged in to the system.
Password Age	Column	The age of the user's password, in days. This lets you know when it is time for users to change their passwords (and remind them if necessary).
Status	Column	The user's current status. Possible values are: • Active – The user is currently active and has access to the system. • Suspend – The user has attempted to log in several times using incorrect log in information and is currently blocked from accessing the system. The user remains locked out until the administrator unlocks the user account. • Timeout – The user has attempted to log in several times using incorrect log in information and is currently blocked from accessing the system for the preconfigured timeout period. The user can either wait for the timeout period to pass or request to be unlocked by the administrator. • Expired – The user can no longer access the system. This often indicates that the user was assigned a temporary role, which allowed access to the system for a limited time. It is recommended to delete any expired user accounts from the system. **Note:** The Audit Trail uses the user's login ID when recording actions performed by this user. When a user account is removed from the system, the system administrator should keep a record (for at least six years) of the personal identity of the user, so that historical data in the Audit Trail can be related to that individual.

3.1.2.2 Groups Tab

In the **Groups** tab you can add, edit, and delete groups and define group settings.



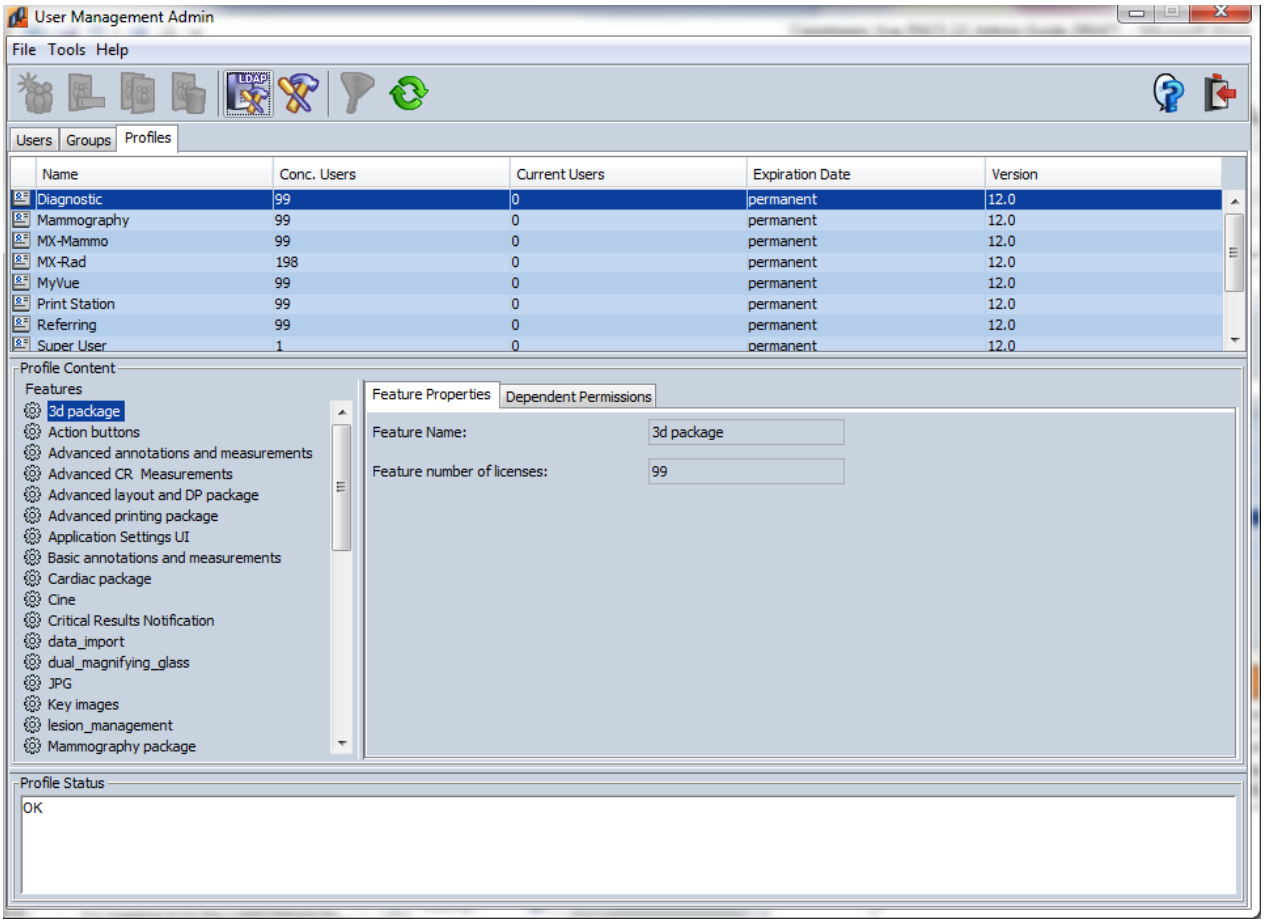
Element	Type	Description
Group Name	Column	The name of the group.
Profile Name	Column	The name of the profile associated with the group. Each profile defines the features a user can use after logging in to the CARESTREAM PACS Client.

3.1.2.3 Profiles Tab

A profile defines the features a user can use in the CARESTREAM PACS Client, where each feature is a licensed permission.

Each group of users has a profile associated with it, and each group has its own set of permissions.

In the **Profiles** tab, you can view the licenses and their associated features.



Element	Type	Description
Name	Column	The name of the profile (license).
Conc. Users	Column	The number of users that can use the license.
Current Users	Column	The number of users currently using the license.
Expiration Date	Column	The expiration date of the license
Version	Column	The version number of the license.
Profile Content		
Features	List	The features included in the profile.
Feature Properties Tab		
Feature Name	Text box	The name of the feature.
Feature number of licenses	Text box	The number of licenses associated with this feature. This is set for a particular feature and overrides the Concurrent Users setting at the profile level.
Dependent Permissions Tab		
Dependent Permissions	List	Indicates whether this feature is dependent on permissions set at the system level.

3.1.3 Configuring the User Management Repository

Before you can start using the User Management Admin tool, you need to perform some initial configuration activities to set the user management repository where the user information is stored.

The following options are available:

- PACS repository—A local PACS repository. This is the default.
- LDAP repository—A central user management repository, such as MICROSOFT Active Directory server.

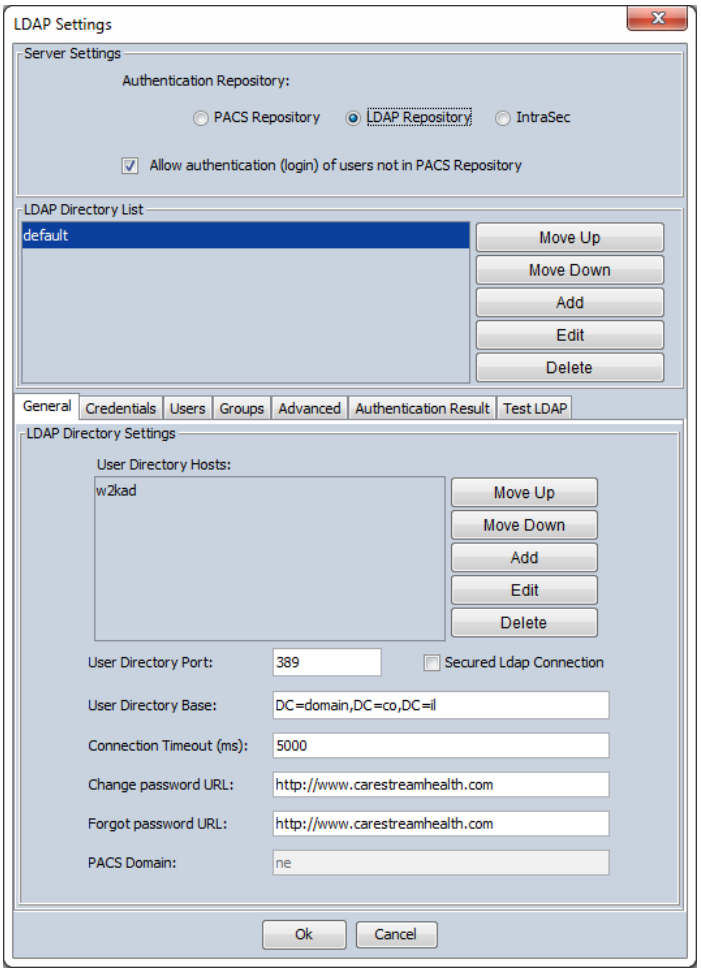
If you are using a central user management repository, you can configure the User Management Admin tool to look up user information using LDAP (Lightweight Directory Access Protocol).

You can set the LDAP configuration to provide the option to create and manage remote PACS users, such as technicians and referring physicians that require limited access to the system, as well as using a central user management repository. These remote PACS users are maintained in a separate domain, without being added to the Active Directory server.

1. In the User Management Admin tool, do one of the following:

   - Click the **LDAP Settings** icon  in the toolbar.
   - From the **Tools** menu, select **Edit LDAP Settings**.

   The **LDAP Settings** window appears.



2. In the **Server Settings** section, select **LDAP Repository** as the authentication repository.
3. If you want to configure the ability to create and manage remote PACS users, select the **Allow authentication (login) of users not in PACS repository** check box.
4. In the **General** tab, do the following:
    a. Click Add to add the server name to the User Directory Hosts list. You can add several hosts to the list and change the order of the host names using the Move Up and Move Down buttons. If failure occurs when connecting to the first host, a second attempt is made to the next host in order, and so on until a connection is made.
    b. In the User Directory Port box, enter the port. There usually are different ports for secured and non-secured connections.
    c. If the LDAP connection is to be secured (SSL), select the Secured LDAP Connection check box.
    d. In the User Directory Base box, enter the Base DN of the LDAP Server user account.
    e. In the Change Password URL box, enter the URL for changing the user password.
    f. In the Forgot Password URL box, enter the URL for changing the password when the user forgets the password.
5. In the **Credentials** tab, do the following:
    a. Select the **Default** option button.
    b. Set the user bind ID and password to be used for the LDAP pre-authentication stage. This setting is used for initial authentication to transform the user login name into an LDAP distinguished name (DN).

    OR

7. If an anonymous bind is to be performed, select the **Anonymous Bind** check box.
6. In the **Users** tab, select the following check boxes:
    - Auto import of LDAP users after successful first login
    - Auto update of LDAP users after successful login
7. In the **Groups** tab, do the following:
    a. Select the Read Security Group from LDAP check box.
    b. In the **Enter Group Attribute Name** box, enter a name for the group attribute.
    c. If required, in the **Group Prefixes** section, click **Add** to add a group prefix to the group name. Any group with a group prefix found in the LDAP server should appear without a prefix in the User Management group list. It should also exist in the User Management application.
8. In the **Advanced Settings** tab, do the following:
    a. From the Search user DN on drop-down list, select Whole subtree starting with Base DN.
    b. In the **Where objectclass** box, type `objectclass=*`.
    c. In the **And attribute** box, type the unique user identifier attribute name. For Active Directory, this is `sAMAccountName`.
    d. Select the Build user DN dynamically check box.

9. In the **Authentication Result** tab, do the following:
    a. In the **Query page size limit** box, enter the page size limit for the LDAP query, for example, `1000`.
    b. From the **Select LDAP query type** drop-down list, select **Paged Query** or **No Paging**, depending on your requirements.
    c. From the Select LDAP error code type drop-down list, select Active Directory Error Codes Only.
10. In the **Test LDAP** tab, enter your user name and password and click **Authenticate to LDAP**.
11. If authentication is successful, a success message appears.

    If authentication fails, an error message appears. You must then reconfigure the LDAP settings until the authentication process is successful.
12. Click **OK** to save your changes and close the window.
13. Restart the system by stopping and then restarting all daemon processes.

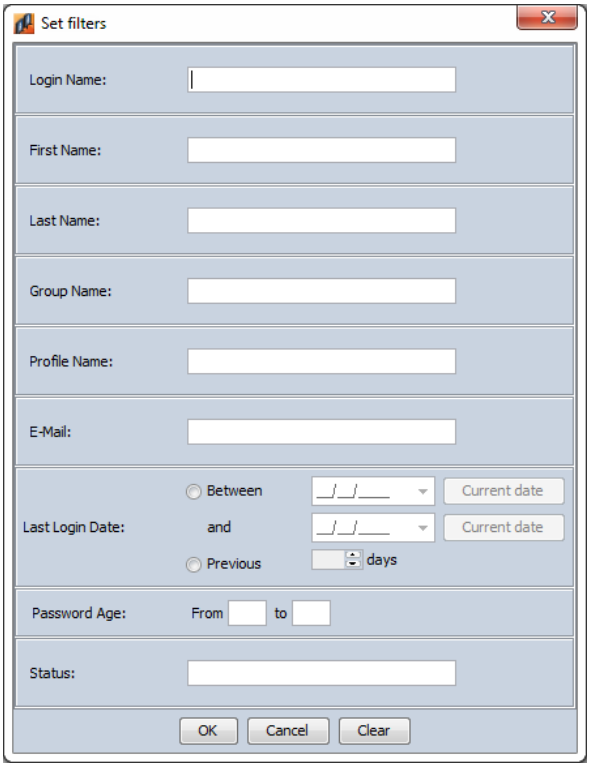
3.1.4 Filtering the Display

You can filter the results shown in the User Management Admin tool according to criteria that you specify. The criteria are different and depend on which tab you are in when you click the **Filter** icon: the **Users** tab or the **Groups** tab.

3.1.4.1 Filtering the Display in the Users Tab

You can filter the results shown in the **Users** tab according to a number of different criteria.

1. In the User Management Admin tool, from the **Users** tab, click the **Filter** icon  in the toolbar.
2. In the **Set Filters** window, enter the desired filter criteria.



3. See Section 4.2.8 User Management Admin Tool Tabs for more information about each of these filter criteria.
4. Click **OK**. The list of users is updated automatically according to the filter criteria specified. In addition, the criteria that the list is currently filtered by appear above the relevant column names.

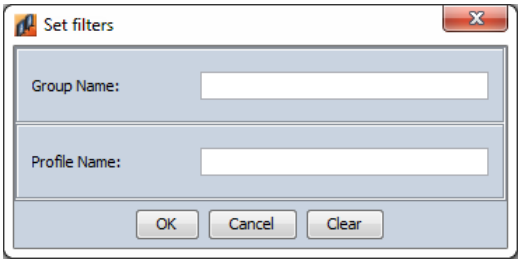
   OR

   Click **Clear** to clear existing filter criteria. You can then reset the filter criteria or click **OK** to close the window.

3.1.4.2 Filtering the Display in the Groups Tab

You can filter the results shown in the **Groups** tab according the group name, the profile name, or both.

1. In the User Management Admin tool, from the **Groups** tab, click the **Filter** icon  in the toolbar.
2. In the **Set Filters** window, enter the desired filter criteria in the **Group Name** box, the **Profile Name** box, or both.



3. Click **OK**. The list of groups is updated automatically according to the filter criteria specified. In addition, the criteria that the list is currently filtered by appear above the relevant column names.

   OR

   Click **Clear** to clear existing filter criteria. You can then reset the filter criteria or click **OK** to close the window.

3.1.5 Sorting the Display

You can sort the results shown in the User Management Admin tool by clicking a column heading. The results are shown in ascending order. Click the same column heading again to sort the results in descending order.

3.1.6 Refreshing the Display

You can refresh the results shown in the User Management Admin tool by clicking the **Refresh** icon  . The results in both the **Users** tab and the **Groups** tab are updated with the latest information.

In addition, the results are sorted in ascending order by Group Name (in the **Groups** tab) and by Login Name (in the **Users** tab).

3.2 Adding New Users and Groups

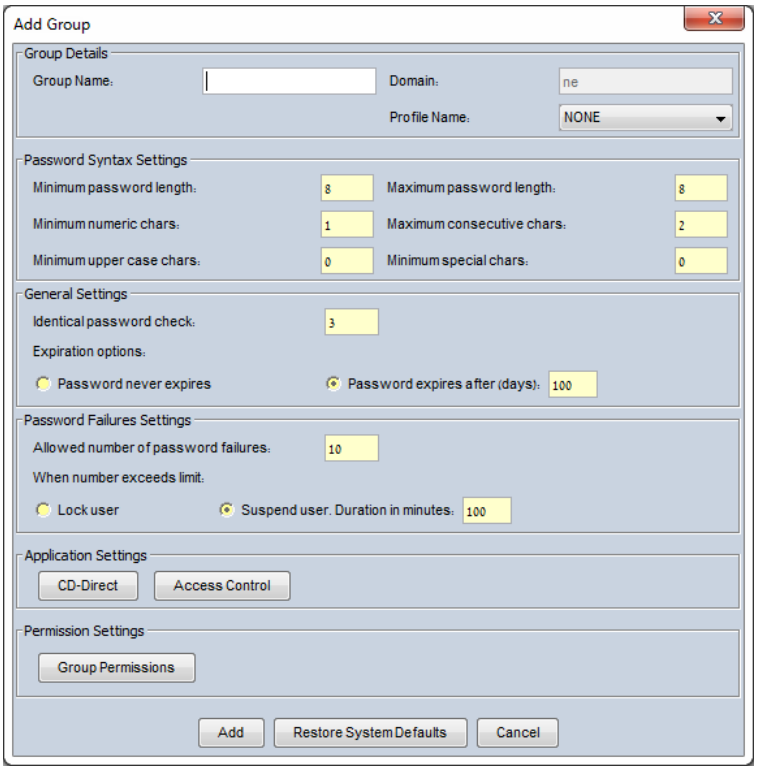
You add new groups to the system and then add users to these groups. In addition, you can also import users from the LDAP repository or from a CSV file.

3.2.1 Adding a Group

When you add a new group to the system, you need to define the group name, as well as the advanced settings that are inherited by each user in the group.

All group details are automatically inherited from the system settings unless you modify them at the group level. Any settings that are modified at the group level override the settings inherited from the system level.

1. In the User Management Admin tool, in the **Groups** tab, do one of the following:
   - Click the **Add New** icon 
   - Select **Add New** from the Tools menu
   - Right-click in the list and select **Add new group**
2. In the **Add Group** window, fill in the following group details:
   - In the **Group Name** box, type a logical name for the group, for example, radiologists.
   - From the **Profile Name** list, select the relevant profile for this group. If you select **NONE**, some features will not be available in the client.



3. In the **Add Group** window, you can do the following:
   - Change the advanced settings that will be inherited by each user in the group. Click **Add** to add the group and close the window.
     See 3.5.4 Advanced Settings for a description of these advanced settings.
   - Click **Restore Group Defaults** to restore any modified files to the default set for the group.
   - Click **Cancel** to close the window without making changes.

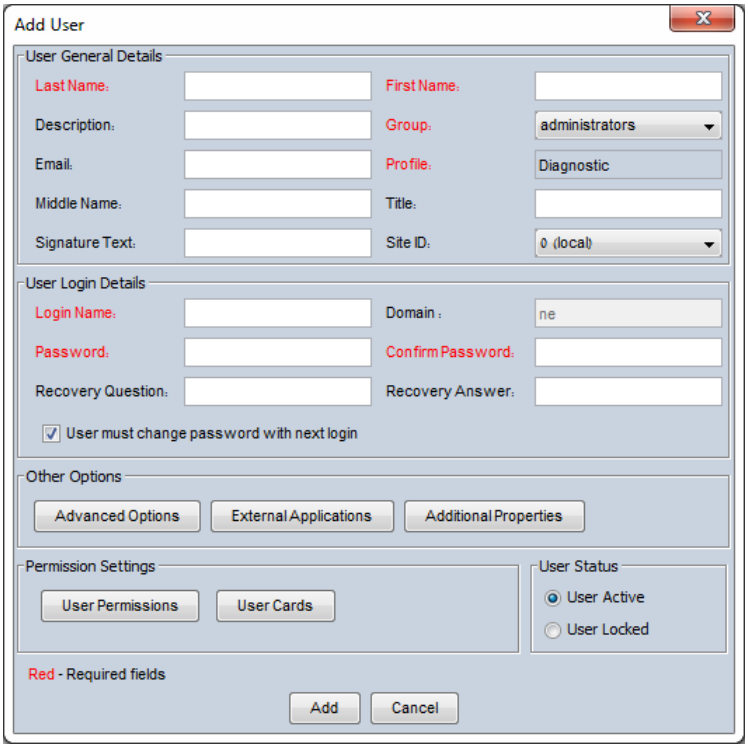
Note: The color of the fields in the **Add Group** window changes according to their status, as follows:

- Yellow indicates that the setting is inherited from the system-level settings.
- White indicates that the value has been modified and is defined at the group level.

3.2.2 Adding a User

When you add a new user to the system, you need to define general and login details, such as the user's name, the name of the group the user is assigned to, and the user's login name and password.

1. In the User Management Admin tool, in the **Users** tab, do one of the following:
   - Click the **Add New** icon  .
   - Select **Add New** from the Tools menu.
   - Right-click in the list and select **Add new user**.
2. In the **Add User** window, fill in the details for the user. Field names in red indicate that the information is mandatory.



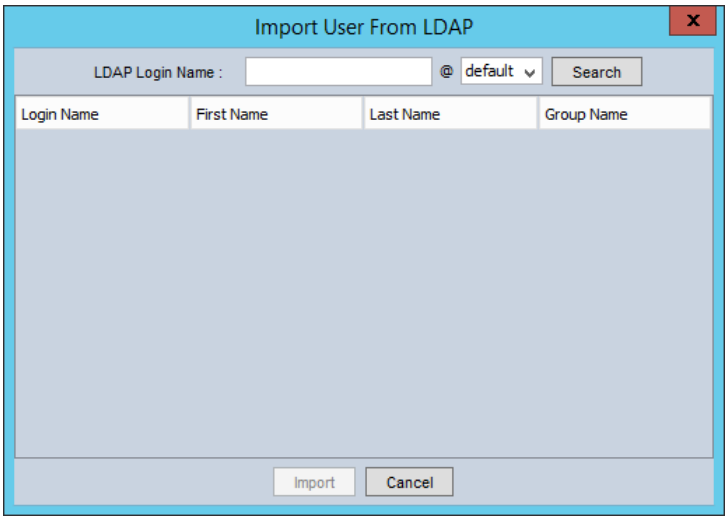
   See Section 3.5.5 Add User and Edit User Settings Window Elements for more information about each of the elements in the **Add User** window.
3. When you have completed the relevant details for a user, click **Add** to close the window. The new user appears in the list of users in the User Management Admin tool.

3.2.3 Importing Users from the LDAP Repository

If you are using a central user management repository, and you want to change the configuration settings for a user, you need to import that user into the User Management Admin tool.

1. In the User Management Admin tool, do one of the following:
   - Click the **Import** icon  in the toolbar.
   - From the **Tools** menu, select **Import**.

2. In the **Import User From LDAP** window, enter the LDAP login name and domain name and click **Search**.



3. Select the user that you want to import and click **Import**. The selected user appears in the list of users in the User Management Admin tool.

3.2.4 Importing Users from a File

You can import users from a CSV file using the `importFromCsv.pl` script, located in:

```
C:\Program Files\Carestream\System5\scripts\
```

The script contains the following flags:

```
AddUsersFromCsv -inputfile=<csv users filename> [-outputdir=<directory name>] [-header]
```

Where:

`AddUsersFromCsv` – Indicates that the CSV file contains a list of users to import

`-inputfile` – The name of the file that contains the user information

`-outputdir` – The location of the log file (optional)

`-header` – Indicates that the first line contains a comma-separated header

If the input file contains a header, use the -header option to notify the program. The default header contains the following fields:

```
last_name,first_name,login,new_password,preferencegroup,domain,email,user_description,question,answer,group_domain_name,middle_name,signature_text,title,user_status,is_expired
```

Note: You can omit columns or leave empty fields, if required.

The password field should be an unencrypted password. If left empty, `12345678` is used.

The `user_status` and `is_expired` fields are internal and should be left empty.

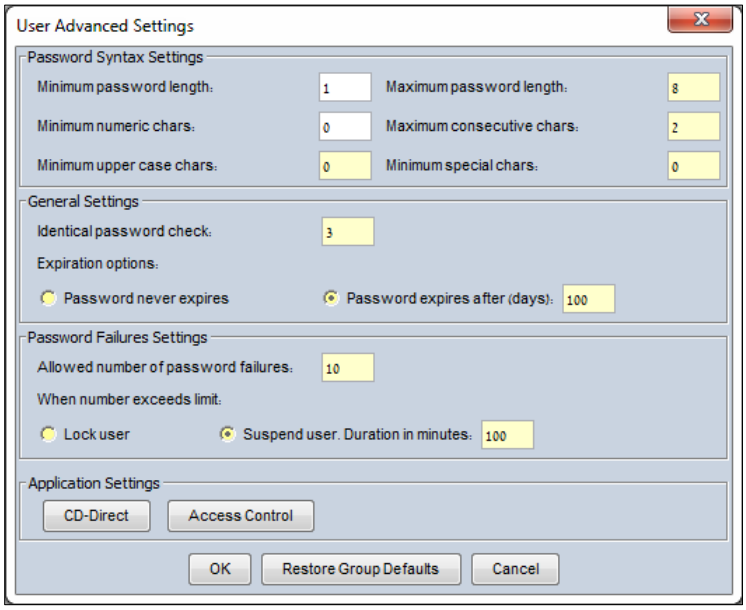
If the first character in the line is #, the line is skipped.

3.3 Defining Advanced Settings for Users

Advanced settings are inherited from the group level, but you can modify them at the user level. Any settings modified at the user level override the settings inherited from the group level.

You define advanced settings for a user when you add the user to the system, or later on by editing the user's settings.

1. In the Add User window or Edit User Settings window, click Advanced Options.
2. In the **User Advanced Settings** window, you can do the following:
   - Change the settings and click **OK**.
     See 3.5.4 Advanced Settings for a description of these advanced settings.
   - Click **Restore Group Defaults** to restore any modified files to the default set for the group, and click **OK**.
   - Click **Cancel** to close the window without making changes.



Note: The color of the fields in the **User Advanced Settings** window changes according to their status, as follows:

- Yellow indicates that the setting is inherited from the group-level settings.
- White indicates that the value has been modified and is defined at the user level.

3.4 Defining External Applications for Users

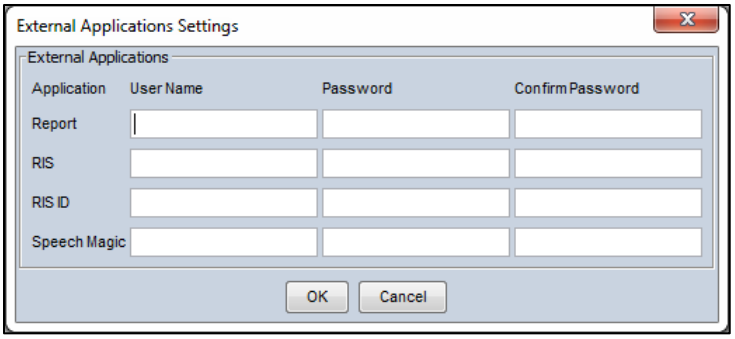
You can define a user's access to external applications, such as RIS or a voice dictation system, so that the user can access the system with a user name and password that is different from that used for the central log in.

This option applies only to Vue PACS Client users. It allows them to access the external system without logging in again, because the login information is automatically refreshed from the User Management Admin Tool.

You define a user's access to external applications when you add the user to the system, or later on by editing the user's settings.

Note: It is not necessary to complete the RIS field when using IS Link as the RIS interface.

1. In the Add User window or Edit User Settings window, click External Applications.
2. In the **External Applications Settings** window, fill in the required user name and password in each of the relevant fields. Re-enter the password to confirm it.



Possible options are:

- **Report**—The user name and password of the user in dictation applications, such as POWERSCRIBE.
- **RIS**— The user name and password of the user in desktop integration with RIS.
- **RIS ID**— The user name field contains the identification of the user (for example – NPI). This is not the user name of the user.
- **Speech Magic**— The user name and password of the user in the SPEECHMAGIC application (used for voice recognition).

3. Click **OK** to close the window.

3.5 Editing Settings at the System, Group, and User Levels

The User Management Admin Tool uses a hierarchical structure of settings at the system, group, and user levels. Each group automatically inherits the default system settings and each user automatically inherits the relevant group settings.

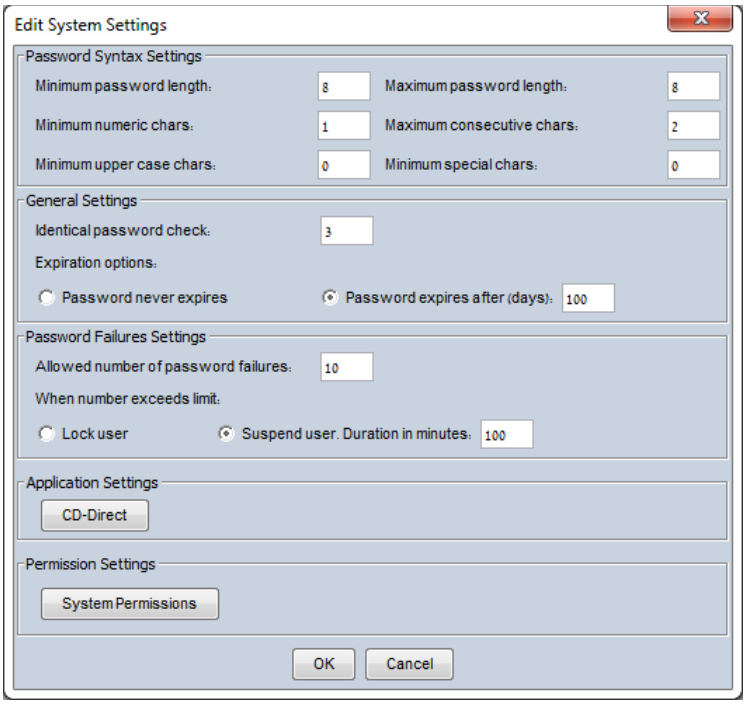
You can override the inherited settings by modifying the values defined for a specific group or user. Any unmodified values remain as is, according to the inherited default system settings.

3.5.1 Modifying the System Settings

You can modify the default system settings that were defined during installation.

The system settings are automatically inherited by the groups and users that you add to the system. You can override the inherited system-level settings at the group level or the user level.

1. In the User Management Admin tool, do one of the following:
   - Click the **Edit System Settings** icon  in the toolbar.
   - From the **Tools** menu, select **Edit System Settings**.
2. In the **Edit System Settings** window, you can do the following:
   - Change the settings and click **OK**.
     See 3.5.4 Advanced Settings for a description of these advanced settings.
   - Click **Cancel** to close the window without making changes.



Note: The Edit System Settings window appears differently depending on whether your system is using LDAP. The options in the Edit System Settings window (with LDAP) are the same as those in the Add Group window except for the Allowed Applications options, which are not relevant at the system level.

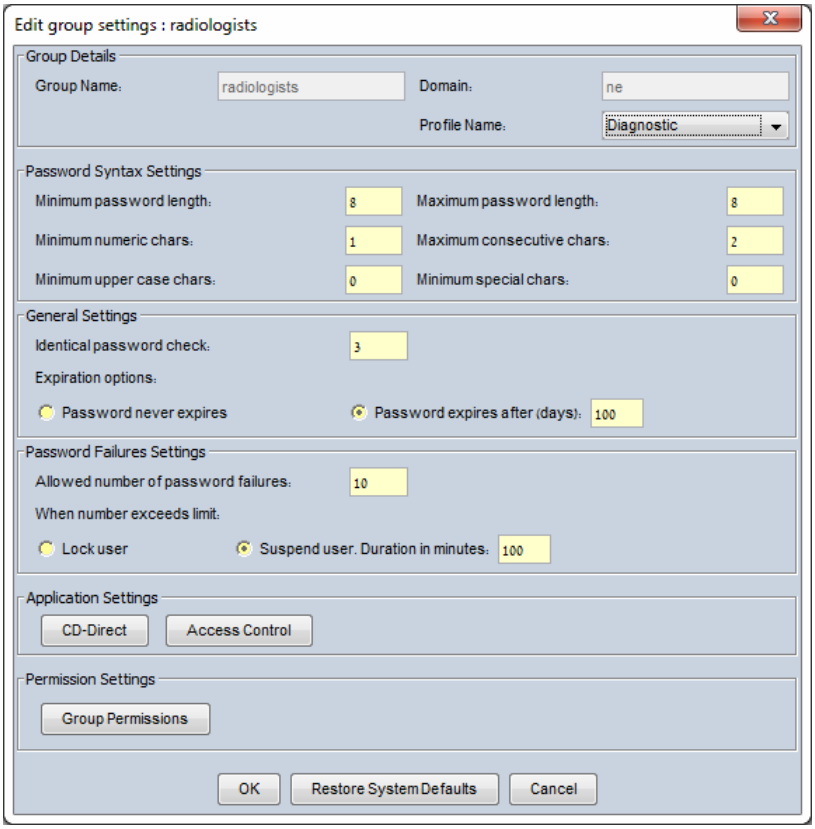
3.5.2 Editing Group Settings

You can modify the advanced settings that are inherited by each user in the group.

1. In the User Management Admin tool, in the **Groups** tab, do one of the following:

   - Click the **Edit selected** icon  .
   - Double-click a group in the list.
   - Select **Edit selected** from the **Tools** menu,
   - Right-click in the list and select **Group properties**.

2. In the Edit Group Settings window, click Group Permissions



Note: The Edit Group Settings window appears differently depending on whether your system is using LDAP.

In addition, the color of the fields changes according to their status, as follows:

- Yellow indicates that the setting is inherited from the system-level settings.
- White indicates that the value has been modified and is defined at the group level.

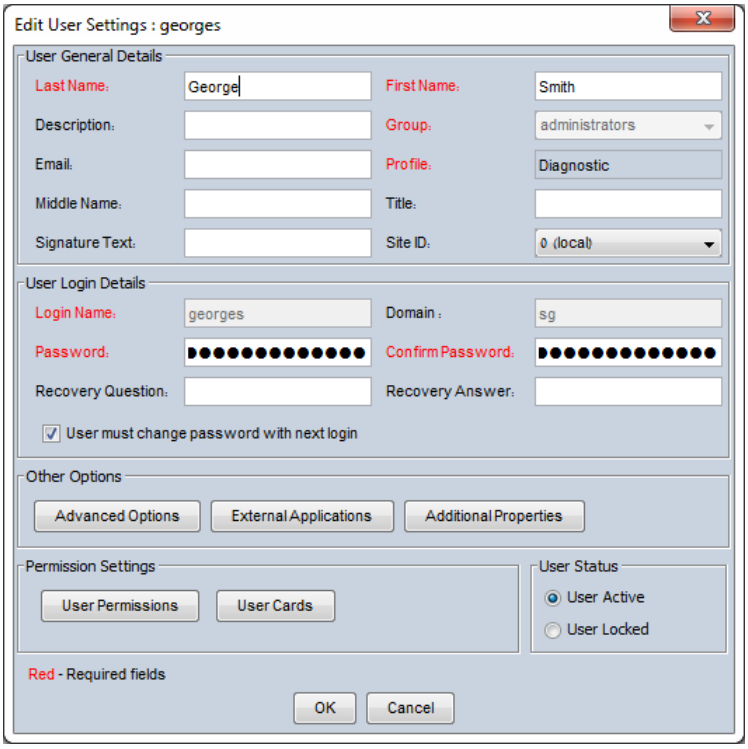
3.5.3 Editing User Settings

You can edit a user's settings, including the general details, login details, and any other advanced settings.

1. In the User Management Admin tool, in the **Users** tab, do one of the following:

   - Click the **Edit selected** icon  .
   - Double-click a user in the list.
   - Select **Edit selected** from the Tools menu.
   - Right-click in the list and select **User properties**.

2. In the **Edit User Settings**, fill in the details for the user. Field names in red indicate that the information is mandatory.

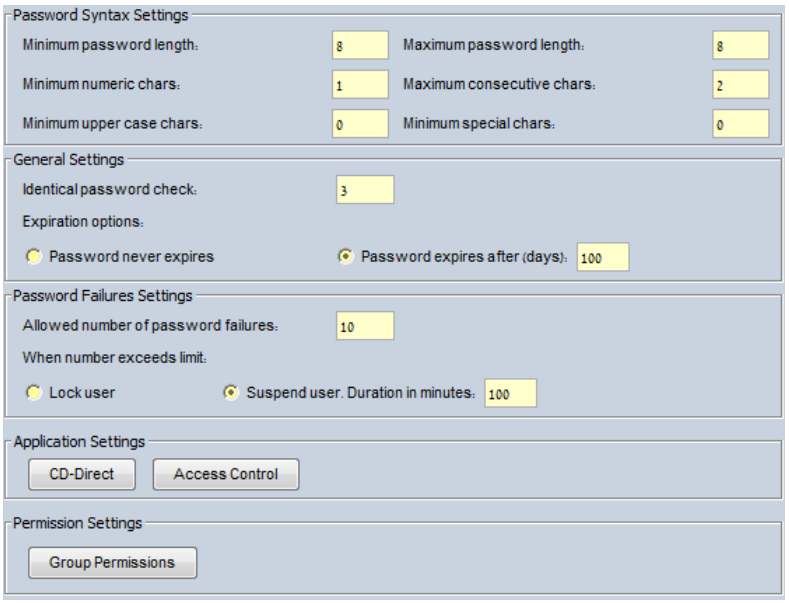


3. See Section 3.5.5 Add User and Edit User Settings Window Elements for more information about each of the elements in the Edit User Settings window.
4. Click OK to close the window.

3.5.4 Advanced Settings Window Elements

The following settings windows include a number of common elements that are described in the table below:

- Add Group
- User Advanced Settings
- Edit System Settings
- Edit Group Settings

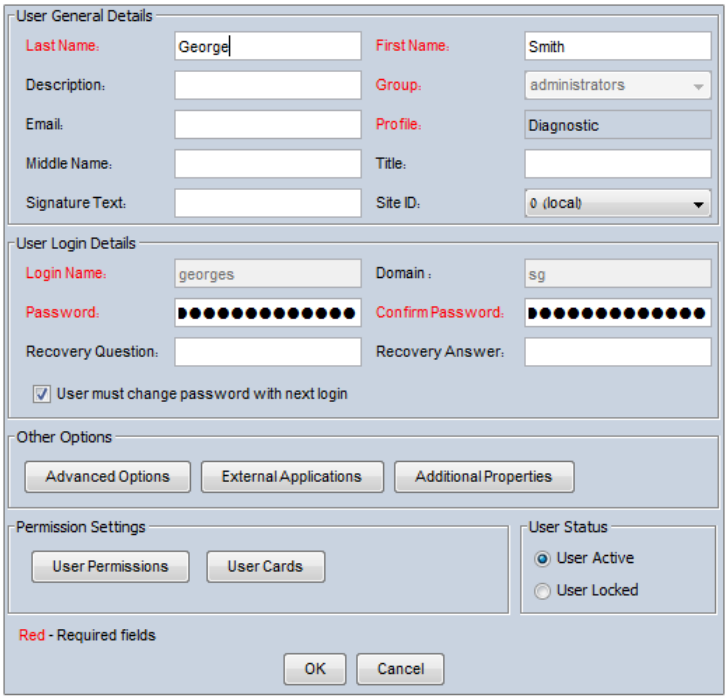


Element	Type	Description
Password Syntax Settings		
Minimum password length	Text box	The minimum number of characters required for each user's password.
Maximum password length	Text box	The maximum number of characters allowed for each user's password.
Minimum numeric chars	Text box	The minimum number of numeric characters required for each user's password.
Maximum consecutive chars	Text box	The maximum number of identical characters allowed in each user's password.
Minimum upper case chars	Text box	The minimum number of upper case characters required for each user's password.
Maximum special chars	Text box	The maximum number of special characters allowed in each user's password.
General Settings		
Identical password check	Text box	The number of passwords that cannot be identical. This prevents the user from using a password that is identical to the previous [x] number of passwords used. For example, if you enter 3, then the user can only use a password if it was not used as one of the last three passwords.

Element	Type	Description
Password never expires	Option button	Select if the password never needs to be changed.
Password expires after (days)	Option button	Select if the password needs to be changed after a set number of days. When the limit is reached, users receive a message that their password has expired and must be changed. You can set the number of days in the adjacent text box.
Password Failures Settings		
Allowed number of password failures	Text box	The number of times a user can enter an incorrect password before being locked out or suspended.
Lock user	Option button	Select to lock the user and prevent access to the system when the limit for entering the incorrect password is exceeded.
Suspend user	Option button	Select to suspend the user for a defined number of minutes when the limit for entering the incorrect password is exceeded.
Duration in minutes	Text box	The amount of time in minutes that the user is suspended when the limit for entering the incorrect password is exceeded.
Application Settings		
CD-Direct	Button	Click to open the **User Default Burner** window in which you can select the default burner for that user or group.
Access Control	Button	Click to open the Access Control window, in which you can assign restrictions at the user, group, or node level. See Section 3.7 Assigning Restrictions to Users and Groups for more information. Appears in the **Add Group**, **User Advanced Settings**, and **Edit Group Settings** windows.
Permission Settings		
System Permissions	Button	Click to open the System Permission Settings window. See 3.8 Modifying Permissions for more information. Appears in the **Edit System Settings** window.
Group Permissions	Button	Click to open the Group Permission Settings window. See 3.8 Modifying Permissions for more information. Appears in the **Add Group** and **Edit Group Settings** windows.

3.5.5 Add User and Edit User Settings Window Elements

The **Add User** and **Edit User Settings** windows include a number of common elements that are described in the table below:



The following table lists the elements that appear in the **Add User** window and the **Edit User Settings** window.

Element	Type	Description
User General Details		
Last Name	Text box	The user's last name. Mandatory field.
First Name	Text box	The user's first name. Mandatory field.
Description	Text box	A textual description relating to the user.
Group	Drop-down list	The group the user is assigned to. Mandatory field.
E-Mail	Text box	The user's email address.
Profile	Text box	The profile assigned to the user. This is assigned automatically when the user is assigned to a group. Mandatory field.
Middle Name	Text box	The user's middle name.
Title	Text box	The user's title.
Signature Text	Text box	The signature text that is used to sign reports.
Site ID	Drop-down list	The site where the user is located.
User Login Details		
Login Name	Text box	The user's assigned log in name.

Element	Type	Description
Domain	Text box	The domain that the user is assigned to.
Password	Text box	A temporary password assigned to the user for the first log in.
Confirm Password	Text box	Confirmation of the password assigned to the user for the first log in.
Recovery Question	Text box	A question that is asked if the user forgets the assigned password. This information must be obtained from the user. **Note:** If a user forgets his or her password and the recovery question is not defined, the user must request a new password from the administrator.
Recovery Answer	Text box	The answer to the recovery question. This information must be obtained from the user.
User must change password with next login	Check box	Select the first time you enter a user's details when you assign a temporary password to the user. The user must then change the password at the first log in. This option is selected by default.
Other Options		
Advanced Options	Button	Click to open the User Advanced Settings window. See Section 3.3 Defining Advanced Settings for Users for more information.
External Applications	Button	Click to open the External Applications Settings window. See Section 3.4 Defining External Applications for Users .for more information
Additional Properties	Button	Click to open the User Additional Properties window in which you can allocate a physician ID to the user.
Permission Settings		
User Permissions	Button	Click to open the User Permission Settings window. See 3.8 Modifying Permissions for more information.
User Cards	Button	Click to open the User Cards Settings window in which you can enter the smart card ID for a user.
User Status		
User Active	Option button	Select to indicate that the user is active and has permission to access and use the system.
User Locked	Option button	Select to indicate that the user is not active and does not have permission to access and use the system. **Note:** This is the manual method for locking or unlocking a user. A locked user is only allowed back into the system after intervention by a system/group administrator or group operator.
Buttons		
Add (Add User window)	Button	Click to add the user and close the window.
OK (Edit User Settings window)	Button	Click to save the changes and close the window.
Cancel	Button	Click to close the window without saving changes.

3.6 Deleting Users and Groups

You can delete users and groups from the system if your assigned role gives you permission to do so. It is recommended to delete users who no longer need to be in the system, for example, users that were assigned a temporary role and now have Expired status.

Note: The Audit Trail uses the user's login ID when recording actions performed by this user. When a user account is removed from the system, you should keep a record (for at least 6 years) of the personal identity of the user, so that historical data in the Audit Trail can be related to that individual.

The following steps describe how to delete a user from the **Users** tab. You can use the same steps to delete a group from the **Groups** tab.

1. In the User Management Admin tool, in the Users tab, do one of the following:
   - Select the user and click the Delete icon  .
   - Select **Delete Selected** from the Tools menu.
   - Right-click the user and select **Delete Selected Users**.
2. In the **Delete Selected User** window, click **OK**. The user is removed from the system and is no longer displayed.

3.7 Assigning Restrictions to Users and Groups

You can restrict user access to Workflow Manager data by assigning restrictions at the user, group, or node level. Then, when a user logs in and requests data, the system automatically checks for restrictions.

A restriction is a combination of the following items:

- Tag – The type of DICOM data that is limited, for example, modality type or body part.
- Value – The value for the specific DICOM tag.

For user-level restrictions, each user must be assigned to a group.

Group-level restrictions are applicable to all users in the group. For example, you can define a CT group and an MRI group and assign a restriction for each group. This limits the groups to view only CT images or only MRI images. You can then assign a specific user to the required group without having to configure specific restrictions for each individual user.

You can use OR and AND operators to add more than one restriction at a time.

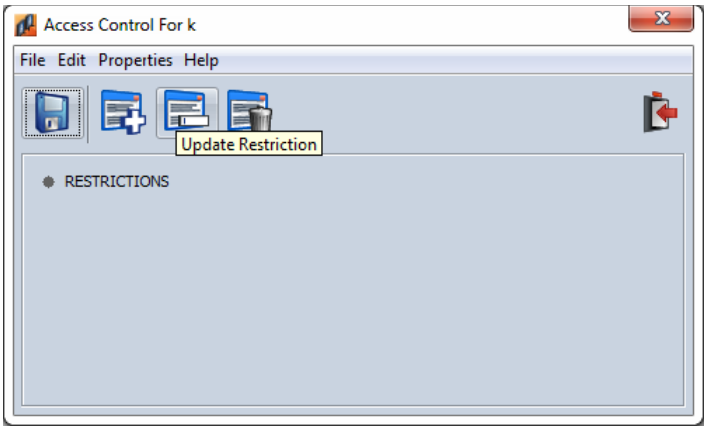
3.7.1 Assigning a Restriction

You assign restrictions in the **Access Control** window, either when adding a new user or group, or by editing an existing user or group. To open the **Access Control** window, click the **Access Control** button in the **User Advanced Settings** window or the **Edit Group Settings** window.

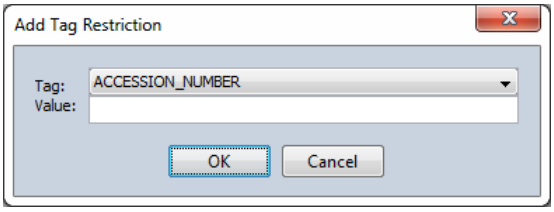
The following steps show how to assign a restriction at the user level. You can use the same procedure to assign a restriction at the group level from the **Edit Group Settings** window.

1. In the User Management Admin tool, in the **Users** tab, select the user to assign the restriction to, and then do one of the following:
   - Click the **Edit selected** icon  .
   - Double-click a user in the list.
   - Select **Edit selected** from the Tools menu,
   - Right-click in the list and select **User properties**.

2. In the Edit User Settings window, click Access Control.
3. In the **Access Control** window, do one of the following:
   - From the Access Control toolbar, click **Add Restriction**  .
   - From the Edit menu, select **Add Restriction**.
   - Right-click in the Tag/Value pane and select **Add Restriction**.



4. In the **Add Tag Restriction** window, do the following:
   - From the Tag drop-down list, select the DICOM tag for the Workflow Manager data that you want to restrict.
   - In the Value field, enter the value for the selected tag.



Note: You can add more than one restriction by inserting a backslash (\) between each value. For example, 1\2 allows the user to access studies from site 1 or 2 only.

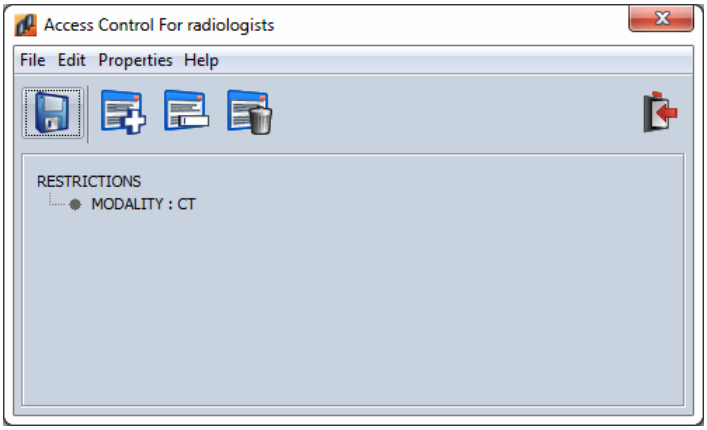
5. Click **OK**. The new access control settings appear in the Tag/Value pane.
6. Repeat steps 3 to 5 to add additional restrictions to the same user, if required.
7. Click Save  .

3.7.2 Updating a Restriction

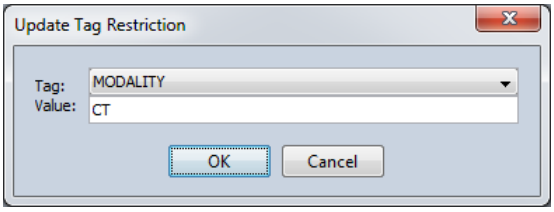
You can update existing restrictions in the Access Control window. For example, you can change the type of data that is limited or you can add additional values to an existing restriction tag. To open the Access Control window, click the **Access Control** button in the **User Advanced Settings** window or the **Edit Group Settings** window.

The following steps show how to update a restriction at the group level. You can use the same procedure to update a restriction at the user level from the **User Advanced Settings** window.

1. In the User Management Admin tool, in the **Groups** tab, select the group to update the restriction for, and then do one of the following:
   - Click the **Edit selected** icon  .
   - Double-click a group in the list.
   - Select **Edit selected** from the Tools menu,
   - Right-click in the list and select **Group properties**.
2. In the **Edit User Settings** window, click **Access Control**. The **Access Control** window appears for the selected group showing any restrictions that have been defined.



3. Select the restriction to update and then do one of the following:
   - From the Access Control toolbar, click **Update Restriction**  .
   - From the Edit menu, select **Update Restriction**.
   - Right-click the restriction and select **Update Restriction**.
4. In the Update Tag Restriction window, do either or both of the following:
   - From the Tag drop-down list, select a different tag for the Workflow Manager data that you want to restrict.
   - In the Value field, enter the value for the new tag or a different value for the existing tag.



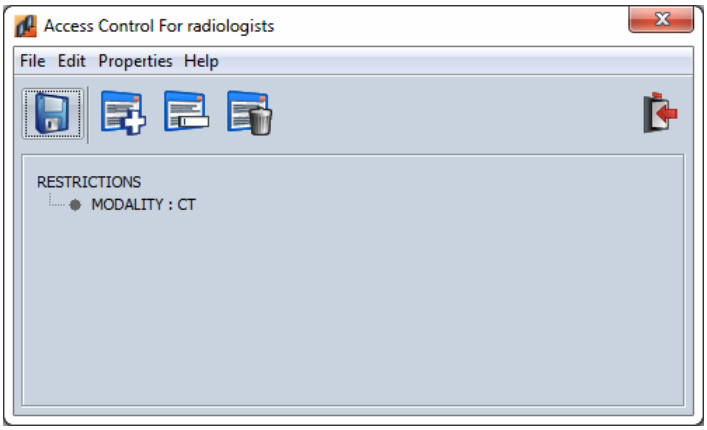
5. Click **OK**. The updated restriction is displayed in the Tag/Value pane.
6. Click **Save**  .

3.7.3 Removing a Restriction

You can remove a restriction from a user or group in the Access Control window. To open the Access Control window, click the **Access Control** button in the **User Advanced Settings** window or the **Edit Group Settings** window.

The following steps show how to update a restriction at the group level. You can use the same procedure to update a restriction at the user level from the **User Advanced Settings** window.

1. In the User Management Admin tool, in the **Groups** tab, select the group to remove the restriction from, and then do one of the following:
   - Click the **Edit selected** icon  .
   - Double-click a group in the list.
   - Select **Edit selected** from the Tools menu,
   - Right-click in the list and select **Group properties**.
2. In the **Edit Group Settings** window, click **Access Control**. The **Access Control** window appears for the selected group showing any restrictions that have been defined.



3. Select the restriction to remove and then do one of the following:
   - From the Access Control toolbar, click **Remove Restriction**  .
   - From the Edit menu, select **Remove Restriction**.
   - Right-click the restriction and select **Remove Restriction/Node**.

   The selected restriction is removed from the Tag/Value pane.
4. Click **Save**  .

3.8 Modifying Permissions

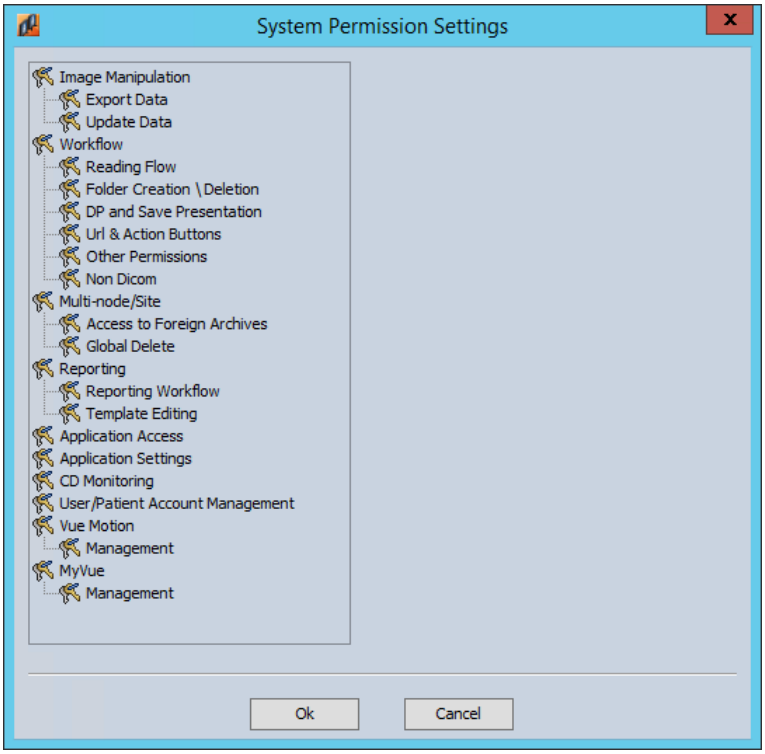
A profile defines the features a user can use in the CARESTREAM PACS Client, where each feature is a licensed permission.

Permissions can be configured at the system, group, or user level, where each level overrides the preceding level.

3.8.1 Modifying System Permissions

System permissions are automatically inherited by any groups and users that you add to the system. You can modify the default system permissions that were defined during installation, or override them at the group level or user level.

1. In the User Management Admin tool, do one of the following:
   - Click the **Edit System Settings** icon  in the toolbar.
   - From the **Tools** menu, select **Edit System Settings**.
2. In the **Edit System Settings** window, click **System Permissions**. The **System Permission Settings** window appears with a list of permissions in the left-hand pane.



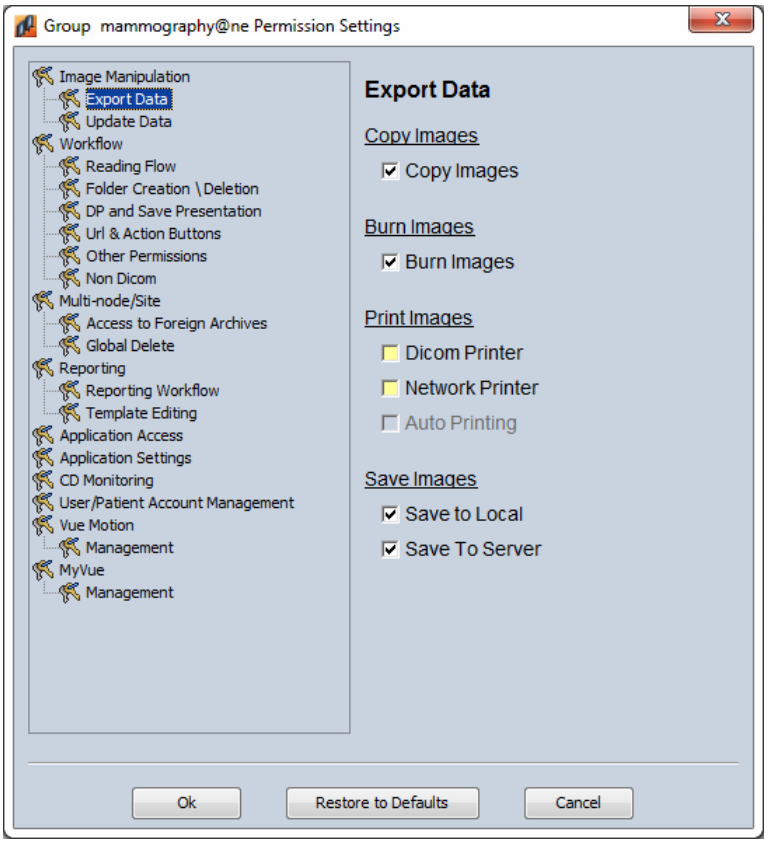
3. Select the relevant permission, and then select the relevant feature check boxes in the right-hand pane. Repeat this action for all relevant permissions.
4. Click **OK** to close the window.

See Section 3.8.4 Permission Settings Window Elements for more information about each of the elements in the **System Permission Settings** window.

3.8.2 Modifying Group Permissions

1. In the User Management Admin tool, in the **Groups** tab, do one of the following:
   - Click the **Edit selected** icon  .
   - Double-click a group in the list.
   - Select **Edit selected** from the **Tools** menu,
   - Right-click in the list and select **Group properties**.

2. In the Edit Group Settings window, click Group Permissions. The Group Permission Settings window opens.



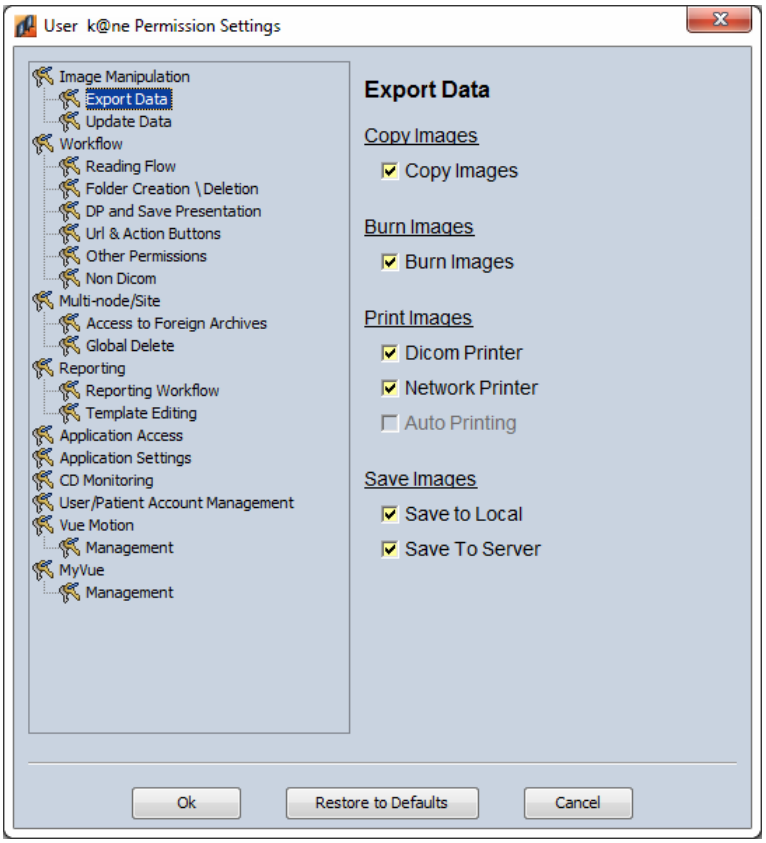
3. Select the relevant permission, and then select the relevant feature check boxes in the right-hand pane. Repeat this action for all relevant permissions.
4. Click **OK** to close the window.

See Section 3.8.4 Permission Settings Window Elements for more information about each of the elements in the **Group Permission Settings** window.

3.8.3 Modifying User Permissions

1. In the User Management Admin tool, in the **Users** tab, do one of the following:
   - Click the **Edit selected** icon  .
   - Double-click a user in the list.
   - Select **Edit selected** from the **Tools** menu,
   - Right-click in the list and select **Group properties**.

2. In the Edit Group Settings window, click User Permissions. The User Permission Settings window opens.



3. Select the relevant permission, and then select the relevant feature check boxes in the right-hand pane. Repeat this action for all relevant permissions.
4. Click **OK** to close the window.

See Section 3.8.4 Permission Settings Window Elements for more information about each of the elements in the **User Permission Settings** window.

3.8.4 Permission Settings Window Elements

The following permissions settings windows include common elements that are described in the tables below:

- System Permission Settings
- Group Permission Settings
- User Permission Settings

3.8.4.1 Image Manipulation Permissions

Element	Type	Description
Export Data		
Copy Images	Check box	Permission to copy images from the local archive to a foreign archive.

Element	Type	Description
Burn Images	Check box	Permission to send data to the CD-Direct Suite. This does not necessarily mean that the user has copy permissions (even though the Info Router uses the copy function for this specific activity).
Print Images	Check box	Permission to print images to a DICOM printer or network printer.
Save Images	Check box	Permission to save data to a local disk or server.
Update Data		
Allow editing patient & study details	Check box	Permission to edit patient and study details. Applies to any update of patient and study details, both in the Archive Explorer (editable fields) and in the Administrator tool (such as update, merge/split, and RIS Sync). Select **Custom fields only** or **Custom and System fields**.
Allow deletion of images & reports	Check box	Permission to delete images and reports. Applies to deletions from the CARESTREAM PACS Client or from the Administration tool.

3.8.4.2 Workflow Permissions

Element	Type	Description
Reading Flow		
Allow Viewing Reports	Check box	Permission to view reports. If this permission is not given, the R or O icons in the Patient Mini-Archive are disabled and the Reports button in the Archive Explorer or the Viewer is disabled. By default, this permission is applied to any user defined in the Radiologists group.
Allow Reading Permissions	Check box	Select from the following check boxes: • Allow Study Status Changes—Permission to move studies from one status to another when clicking **Done**, and to lock a study. If permission is not granted, the user returns to the Archive Explorer when clicking **Done**. • Allow Dictation Permission—Permission to dictate a report. • Allow Saving Reports—Permission to save reports automatically generated in CARESTREAM PACS applications, such as Calcium Scoring and Vessel Analysis. • Allow Creating Critical Result Notification—Permission to create a critical result notification. By default, these permissions are applied to any user that is defined in the Radiologists group.
Allow Marking Key Images	Check box	Permission to mark images as key images. Only users with reading permissions can be assigned this permission. By default, this permission is applied to any user defined in the Radiologists group. **Note:** The permission to mark key images does not necessarily mean that the user has Save As permissions. Users who do not have permission to Save Images to Server can still mark key images.
Allow Marking Significant Series	Check box	Permission to mark images as a significant series. Only users with reading permissions can be assigned this permission. By default, this permission is applied to any user defined in the Radiologists

Element	Type	Description
		group.
Allow Unmarking Significant Series	Check box	Permission to unmark images that were previously marked as a significant series. Only users with reading permissions can be assigned this permission. By default, this permission is applied to any user defined in the Radiologists group.
Allow Updating Critical Result Status	Check box	Permission to update the critical result status of a study. Only users with reading permissions can be assigned this permission. By default, this permission is applied to any user defined in the Radiologists group.
Sticky Notes	Drop-down list	The levels of permission for sticky notes: • None • View Only • View, Add • View, Add, Edit, Delete user's own • View, Add, Edit, Delete (no restriction)
Teaching Files	Drop-down list	The levels of permission for teaching files: • View Only • View, Add • View, Add, Edit, Delete user's own • View, Add, Edit, Delete (no restriction)
Allow Modifying Teaching File Forms	Check box	Permission to modify a teaching file form.
Folder Creation/Deletion		
Regular Folders	Check box	Permission to create and delete regular folders. Select the **Private** or **Public** option button.
Worklist Folders	Check box	Permission to create and delete Worklist folders. Select the **Private** or **Public** option button.
Teaching Folders	Check box	Permission to create and delete Teaching folders. Select the **Private** or **Public** option button.
Allow Saving of Default Folder Settings	Check box	Permission to save the default folder settings.
DP and Save Presentation		
DP Creation Permissions	Check box	Permission to create, edit, and delete user, group, and system display protocols (DPs) by using Save As and the DP Editor. Also allows use of the DP repair tool. Can be applied only to users who have permission to create, edit, and delete system display protocols using the DP Editor. By default, this permission is applied to any user defined in the System Administrators group.
Save Presentation Permissions	Check box	Permission to create, edit, and delete presentations for a study. By default, this permission is applied to any user defined in the Radiologists group.

Element	Type	Description
URL and Action Buttons		
Allow viewing additional studies after URL activation	Check box	Permission to change a study after the URL activation is invoked (launch Archive Explorer and select a different study). **Note:** The permission to allow URL activation is included under the Application Access Permissions.
Default Action Button Permissions	Drop-down list	Permission to activate a specific action button that is configured on site (for example, the ORTHOVIEW action button triggering the integration with the ORTHOVIEW application). Possible values are **Allow** or **Not Allow**.
Other Permissions		
Allow login as another user to CS Client	Check box	Permission to log in to the client as another user.
Allow Clearing Studies from Local Drive	Check box	Permission to clear studies from the local drive.
Allow Pushing Studies to Other Users than Myself	Check box	Permission to push studies to other users.
Allow modifying My Tab, right-click menu and shortcuts	Check box	Permission to modify My Tab, right-click menu and shortcuts.
Non-DICOM		
Allow Access to the following sites	Check box	Permission to allow access to the following cases for non-DICOM images: • User's site cases • Specific cases • All cases

3.8.4.3 Multi-node/Site Permissions

Element	Type	Description
Access to Foreign Archives		
<remote server>	Drop-down list	Permission to read, write and delete images to/from the configured remote servers.
Default Device Permissions	Drop-down list	Permission to read, write and delete images to/from the default device.
Allow Global Access For Patient History	Check box	Permission for global access to patient history.
Global Delete		
Allow Synchronization of Images/Reports deletions with the following site-ids	Check box	Permission to synchronize images and reports deleted from the configured sites.

3.8.4.4 Reporting Permissions

Element	Type	Description
Reporting Workflow		
Allow Integrated Reporting	Check box	Permission to perform integrated reporting. Select from the following options: For radiologists: • Speech Recognition • Dictation Only • Typing Only For transcriptionists: • Transcription
Allow Signing Without Password	Check box	Permission to sign a report without a password.
Allow Addendum Creation	Check box	Permission to create an addendum. You can also allow a user to create an addendum for another user's report.
Allow Signing Other User's Draft Reports	Check box	Permission to sign another user's draft report.
Allow Report Creation Without Study	Check box	Permission to create a report without an associated study.
Allow Loading Images	Check box	Permission to load images to a report.
Allow Batch Signing	Check box	Permission to batch sign a number of reports.
Allow Digital Signature for Other User's Report	Check box	Permission to sign another user's report.
Template Editing		
Allow Templates/Auto-Texts Creation	Check box	Permission to create templates and auto-texts. Select the **User**, **Group**, or **System** option.
Allow Changing The System Default Template	Check box	Permission to change the default template.
Allow Changing The System Addendum Template	Check box	Permission to change the addendum template.
Allow Changing The System Master Template	Check box	Permission to change the master template.

3.8.4.5 Application Access Permissions

Element	Type	Description
<application>	Check box	Permission to access the following applications: • Carestream Client • Carestream Client via URL activation • Carestream Client via COM interface • Carestream Vue Motion • Carestream MyVue • Vue Explorer • CD-Direct • Data Import Tool • System Configuration • System Administration • System Monitoring • User Management Admin • Central Configuration

3.8.4.6 Application Settings Permissions

Element	Type	Description
Allow UI & Viewing Settings	Check box	Permission to access the user interface and viewing settings. Select the **User**, **Group**, or **System** option.
Allow True Size Calibration	Check box	Permission to perform true size calibration.
Allow Printing Calibration	Check box	Permission to perform printing calibration.
Allow Reports & 3rd Party Settings	Check box	Permission to generate reports and access third-party settings.

3.8.4.7 CD Monitoring Permissions

Element	Type	Description
Allow updating user's burn requests in queue	Check box	Permission to update a user's queued burn requests.
Allow updating CD-Direct settings	Check box	Permission to update the CD-Direct settings.

3.8.4.8 User/Patient Account Management Permissions

Element	Type	Description
General User Management		
Allow add/edit/delete users	Check box	Permission to add, edit, and delete users. Select the **Group** or **System** option.

Element	Type	Description
Allow resetting user's passwords	Check box	Permission to reset user passwords. Select the **Group** or **System** option.
Web User Management		
Allowed Actions	Drop-down list	Defines the allowed actions for Web users. Possible values are: • None • Create, Edit Only • Create, Edit, Delete
Share exams with 'Other' Web Users	Check box	Permission to share exams with other Web users.

3.8.4.9 Vue Motion Permissions

Element	Type	Description
Save to Local	Check box	Permission to save studies to a local directory.
Send Study	Check box	Permission to send a study.
Allow Viewing Reports	Check box	Permission to view reports.
Print Reports	Check box	Permission to print reports. Only relevant if the Allow Viewing Reports check box is selected.
Free Search	Check box	Permission to perform a free search on studies.
Allow Order Entry	Check box	Permission to perform order entry.
Allow modification of patient details	Check box	Permission to modify patient details.
Allow Management of Referring Physicians Lookup Table	Check box	Permission to manage the Referring Physicians lookup table.
Advanced Viewer	Check box	Permission to use the Advanced Viewer.
Allow viewing additional studies after URL activation	Check box	Permission to view additional studies after URL activation.
Vue Motion 3D renditions	Check box	Permission to perform 3D renditions in Vue Motion.
Sticky Notes	Drop-down list	The levels of permission for sticky notes: • None • View Only • View, Add • View, Add, Edit, Delete user's own • View, Add, Edit, Delete (no restriction)

3.8.4.10 MyVue Permissions

Element	Type	Description
Carestream MyVue	Check box	Permission to use CARESTREAM MyVue.
Share Data	Check box	Permission to share data.
Save to Local	Check box	Permission to save studies to a local directory.
Allow Viewing Reports	Check box	Permission to view reports.
Print Reports	Check box	Permission to print reports. Only relevant if the **Allow Viewing Reports** check box is selected.

4 Performing System Configuration

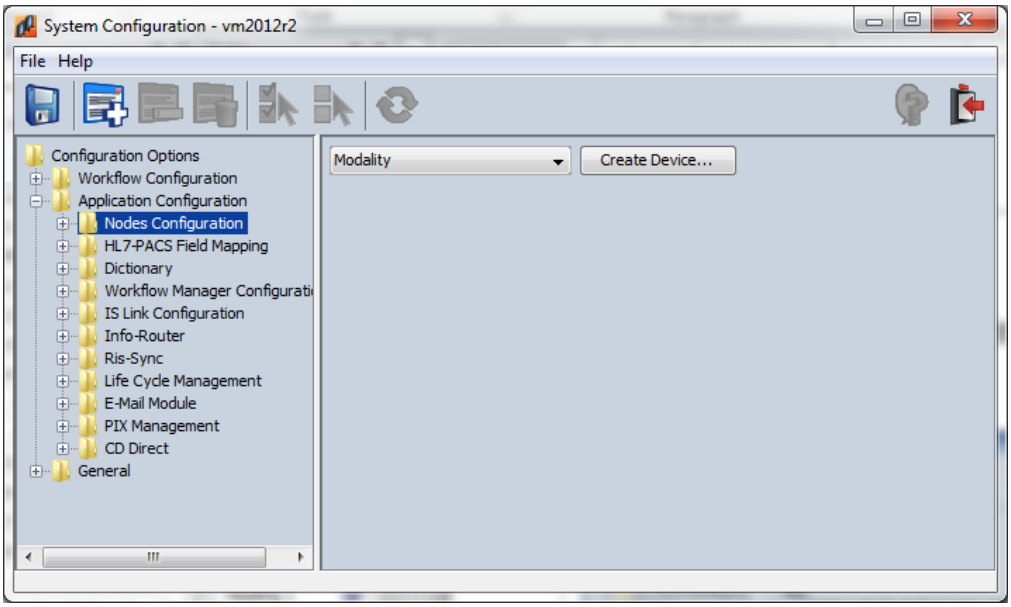
You can use the System Configuration tool to configure and tune the system according to your site's requirements. Proper configuration enhances system performance and saves time and resources.

You can use the System Configuration tool for the following activities:

- Configuring Devices
- Updating the Workflow Manager Node Configuration
- Configuring the Workflow Manager
- Configuring IS Link
- Configuring HL7-PACS Field Mapping
- Configuring the Info Router
- Configuring RIS Synchronization
- Configuring Life Cycle Management
- Configuring Patient Matching Rules

4.1 Getting Started with the System Configuration Tool

To open the System Configuration tool, select **System Configuration** from the Administration Tool menu. The System Configuration tool opens showing the configuration options in the left pane.



4.1.1 Using the System Configuration Toolbar

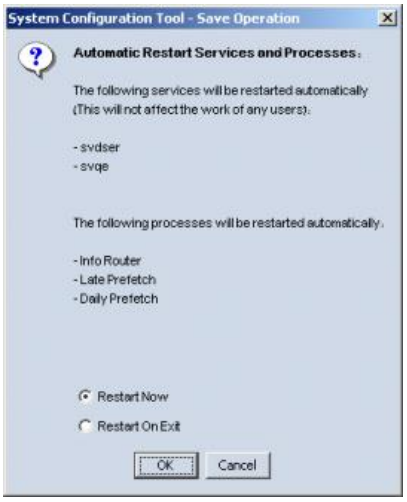
#	Description
1	**Save**—Click to save your changes
2	**Add**—Click to add a new item
3	**Edit**—Click to edit the selected item
4	**Delete**—Click to delete the selected item
5	**Select All**—Click to select all items
6	**Select None**—Click to remove selections
7	**Refresh**—Click to refresh the display with the latest information
8	**Help**—Not in use
9	**Exit**—Click to close the application

The System Configuration toolbar is page-sensitive; when toolbar functions are not relevant to a particular page, they are grayed out.

4.1.2 Saving Your Changes

When you have made changes in the System Configuration tool, you need to save the changes and restart the affected services.

When you finish setting configuration parameters, the **Save Operation** window appears showing the changes made and the restart options. Both services and processes can be restarted. You can choose to restart immediately or on exit.



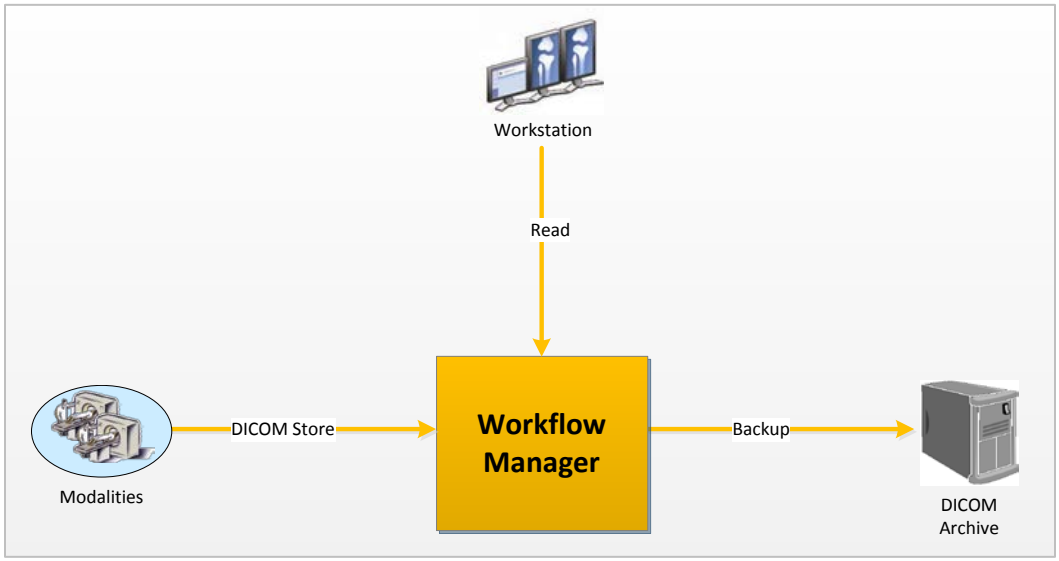
4.2 Configuring Devices

Medical imaging applications and devices connected to a hospital network usually exchange information using the DICOM protocol. Each of these devices is known as an application entity (AE) and each application entity has its own unique name, known as an AE title.

Devices that communicate using the DICOM protocol are also known as DICOM nodes or DICOM peers.

When you configure devices in your network, you must define their static IP address and port, so that the devices can communicate. You can also define additional optional settings depending on the type of device.

The following figure illustrates a typical hospital network, where modalities, a workstation and a DICOM archive are connected to the Workflow Manager.



In the System Configuration tool, you use the **Nodes Configuration** option to configure the following devices:

- Modality
- DICOM printer
- DICOM archive
- Workstation
- Reporting
- Remote Web portal

4.2.1 Configuring Modalities

You can configure modalities in one of two ways:

- When you have a large number of modalities to configure, for example, when you set up a new hospital network with 500 modalities, you can set the allowed net addresses that the Workflow Manager can receive. For example, all modalities with an IP that starts with 192.168 can send DICOM images to the Workflow Manager.
- When you have a single or small number of modalities to configure, for example, when an already-configured modality is not working properly and you would like to configure it manually, or when you add a new modality to the network with a network that you do not wish to allow.

4.2.1.1 Configuring a Large Number of Modalities

When you have a large number of modalities to configure, use the **Allowed Net** option to set the allowed net addresses from which the Workflow Manager can receive DICOM images.

See Section 4.3.2 Specifying Allowed and Forbidden Hosts for more information.

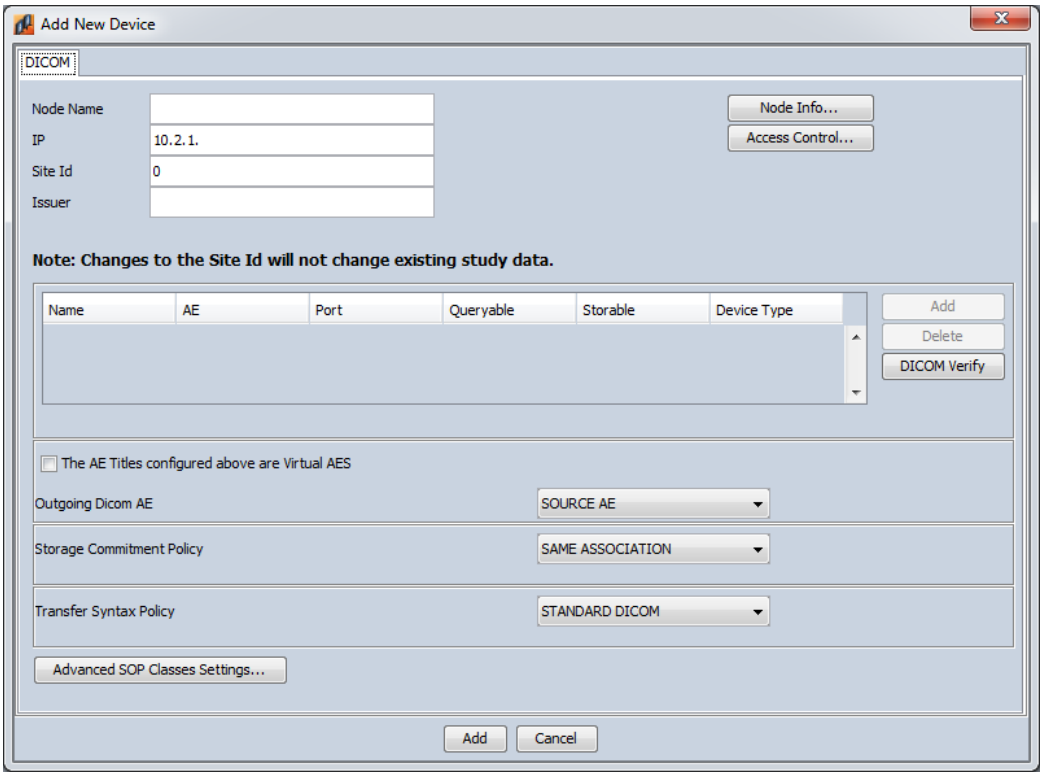
4.2.1.2 Configuring a Single Modality

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration**.
2. In the right pane, select **Modality** and click **Create Device**.

   OR

   Right-click **Nodes Configuration** and select **Add**.

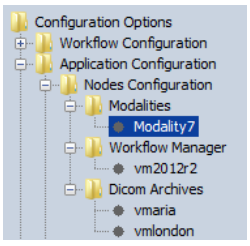
   The **Add New Device** window appears.



   Enter values for the following mandatory fields:

   - **Node Name**
   - **IP**
   - **Issuer**

3. Click **Add**. The new modality appears in the left pane under the Modalities node.



4. In the **AE Titles** section, type the AE Title name. This is the unique name that identifies the device to other DICOM entities on the network.

   Note: The AE title is case sensitive and has a maximum of 16 characters.

5. Leave the other elements in the **Add New Device** window with their default values, or change them according to your requirements.

   See Section 4.2.8 Add New Device Window Elements for more information about each of the elements in the **Add New Device** window.

6. Click **Save**  , then restart the affected services.

You now need to verify the connection to the modality. See Section 4.2.7 Verifying the DICOM Connection for more information.

4.2.2 Configuring a DICOM Printer

You can configure a DICOM printer to print DICOM images on X-ray film and paper.

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration**.
2. In the right pane, select **DICOM Printer** and click **Create Device**.

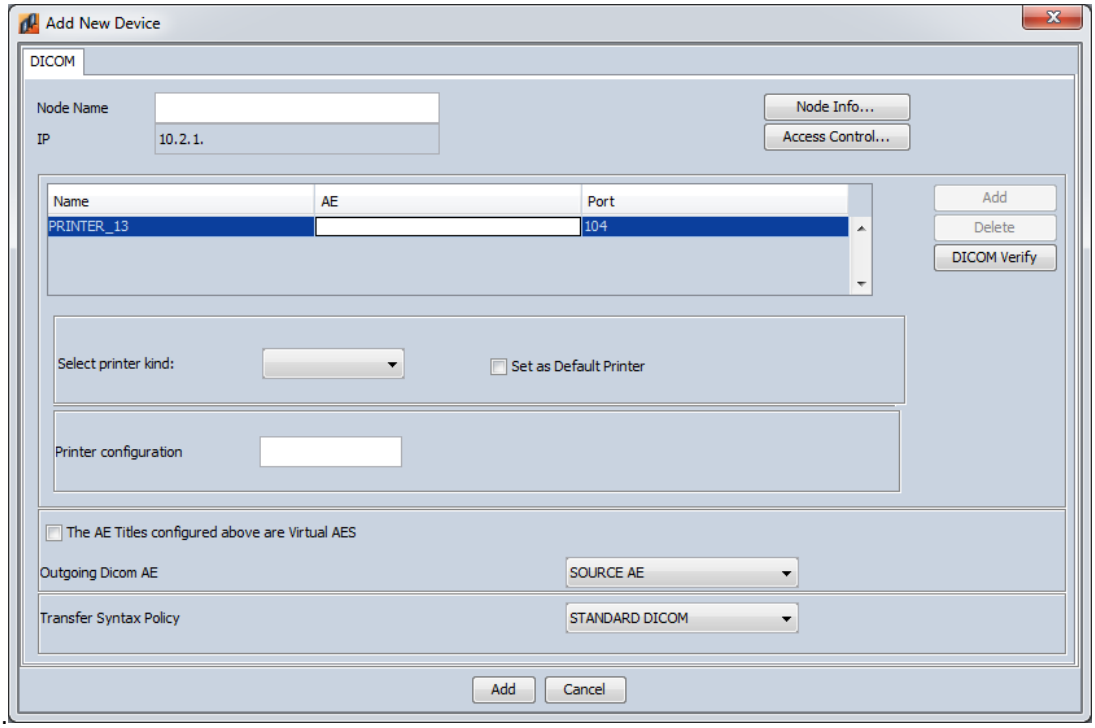
   OR

   Right-click **Nodes Configuration** and select **Add**.

   The **Add New Device** window appears.

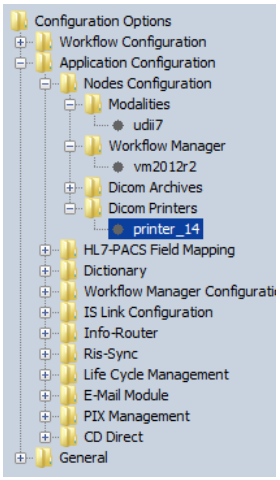
   Note: The **AE titles** section appears partiality populated with default values.

3. Click anywhere in AE titles section. The **Add New Device** window expands to include the **Select printer** drop-down list and **Printer configuration** box.



4. Enter values for the following mandatory fields:
    - **Node Name**
    - **IP**
5. In the **AE Titles** section, type the AE Title name. This is the unique name that identifies the device to other DICOM entities on the network.

    Note: The AE title is case sensitive and has a maximum of 16 characters.
6. From the **Select printer kind** drop-down list, click the printer type to be added.
7. To set this printer as the default printer, select the **Set as Default Printer** check box.
8. If the printer uses implementation-specific print parameters, type the values in the **Printer configuration** box.
9. Click **Add**. The new printer appears in the left pane under the DICOM Printers node.



10. Leave the other elements in the **Add New Device** window with their default values, or change them according to your requirements.

    See Section 4.2.8 Add New Device Window Elements for more information about each of the elements in the **Add New Device** window.
11. Click **Save**  , then restart the affected services.

You now need to verify the connection to the printer. See Section 4.2.7 Verifying the DICOM Connection for more information.

You also need to configure the DICOM printer in the client workstation.

4.2.3 Configuring a DICOM Archive

You can configure a DICOM archive as a DICOM node.

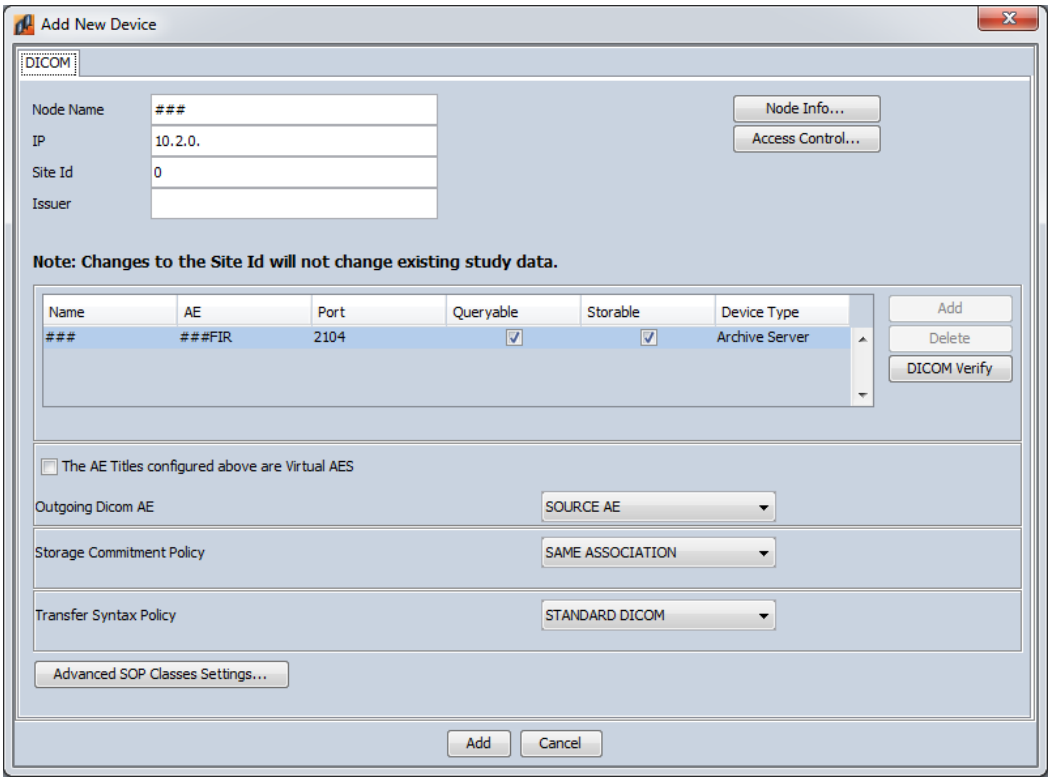
1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration**.
2. In the right pane, select **DICOM Archive** and click **Create Device**.

    OR

    Right-click **Nodes Configuration** and select **Add**.

    The **Add New Device** window appears.

    Note: The **AE titles** section appears partiality populated with default values.



3. Enter values for the following mandatory fields:
   - **Node Name**
   - **IP**
   - **Issuer**

   Note: The Name and AE title in the **AE titles** section are automatically populated with the node name.
4. Click **Add**. The new archive appears in the left pane under the DICOM Archives node.
5. Leave the other elements in the **Add New Device** window with their default values, or change them according to your requirements.

   See Section 4.2.8 Add New Device Window Elements for more information about each of the elements in the **Add New Device** window.
6. Click **Save**  , then restart the affected services.

You now need to verify the connection to the archive. See Section 4.2.7 Verifying the DICOM Connection for more information.

4.2.4 Configuring a Workstation

You can configure a diagnostic workstation as a DICOM node.

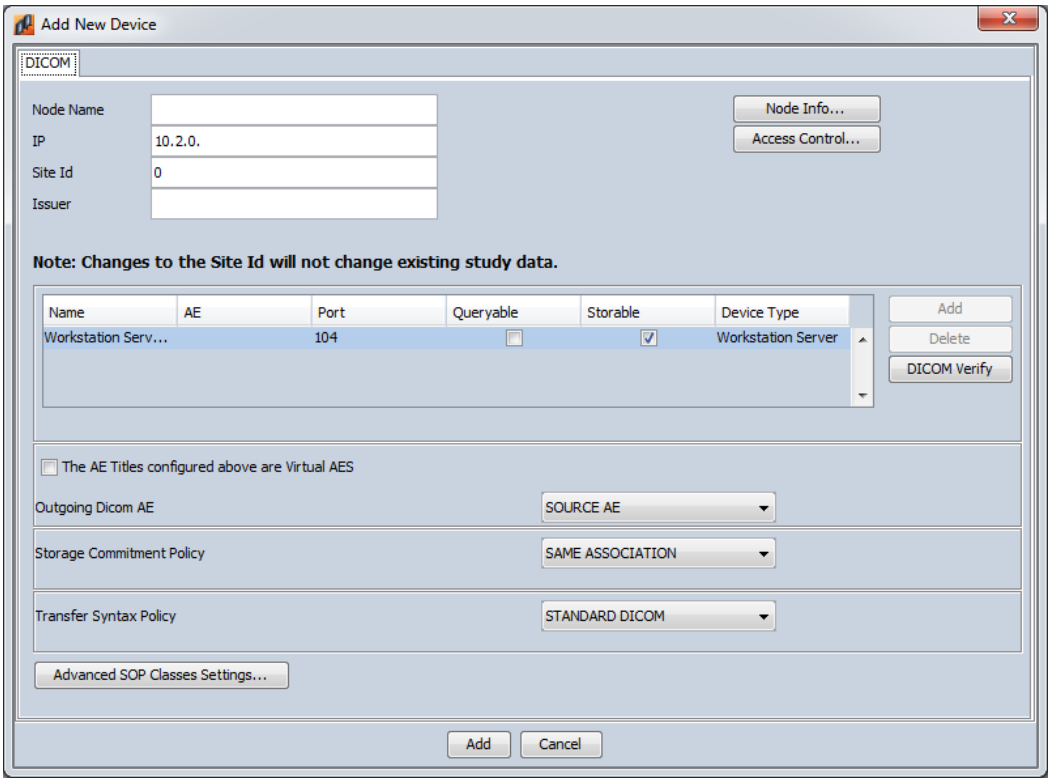
1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration**.
2. In the right pane, select **Workstation** and click **Create Device**.

   OR

   Right-click **Nodes Configuration** and select **Add**.

The **Add New Device** window appears.

Note: The **AE titles** section appears partiality populated with default values.



3. Enter values for the following mandatory fields:
   - **Node Name**
   - **IP**
   - **Issuer**
4. In the **AE Titles** section, type the AE Title name. This is the unique name that identifies the device to other DICOM entities on the network.

   Note: The AE title is case sensitive and has a maximum of 16 characters.
5. Click **Add**. The new workstation appears in the left pane under the Workstation node.
6. Leave the other elements in the **Add New Device** window with their default values, or change them according to your requirements.

   See Section 4.2.8 Add New Device Window Elements for more information about each of the elements in the **Add New Device** window.
7. Click **Save**  , then restart the affected services.

You now need to verify the connection to the workstation. See Section 4.2.7 Verifying the DICOM Connection for more information.

4.2.5 Configuring Reporting

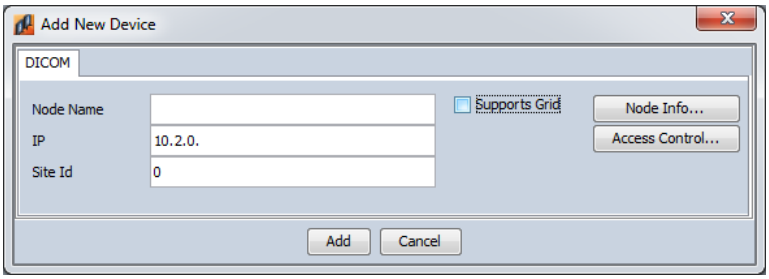
You can configure the Speech Server as a Reporting node.

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration**.
2. In the right pane, select **Reporting** and click **Create Device**.

   OR

   Right-click **Nodes Configuration** and select **Add**.

   The **Add New Device** window appears.



3. Enter values for the following mandatory fields:
   - **Node Name**
   - **IP**
4. If the Speech Server is part of a grid network, select the **Supports Grid** check box. Then complete the relevant grid details in the **Grid** tab that appears.

   See Section 4.2.8 Add New Device Window Elements for more information about each of the elements in the **Add New Device** window.
5. Click **Add**. The Speech Server appears in the left pane under the Reporting node.
6. Click **Save**  , then restart the affected services.

You now need to verify the connection to the Speech Server. See Section 4.2.7 Verifying the DICOM Connection for more information.

4.2.6 Configuring a Remote Web Portal

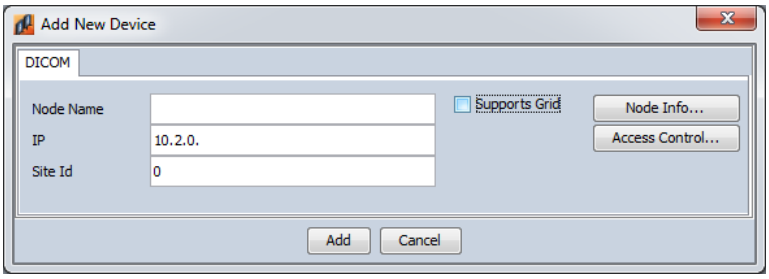
You can configure a remote Web portal for Vue Motion.

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration**.
2. In the right pane, select **Remote Web Portal** and click **Create Device**.

   OR

   Right-click **Nodes Configuration** and select **Add**.

   The **Add New Device** window appears.



3. Enter values for the following mandatory fields:
    - **Node Name**
    - **IP**
4. If the Web application is part of a grid network, select the **Supports Grid** check box. Then complete the relevant grid details in the Grid tab that appears.

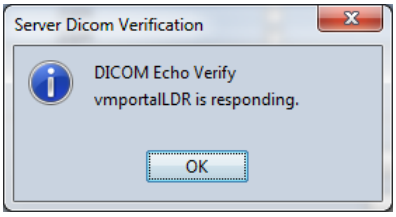
    See Section 4.2.8 Add New Device Window Elements for more information about each of the elements in the **Add New Device** window.
5. Click **Add**. The application appears in the left pane under the Remote Web Portals node.
6. Click **Save**  , then restart the affected services.

You now need to verify the connection to the remote Web portal. See Section 4.2.7 Verifying the DICOM Connection for more information.

4.2.7 Verifying the DICOM Connection

When you have finished configuring a device, you need to verify the connection to it.

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration**.
2. Select the device that you want to verify the DICOM connection for.
3. In the right pane, if there is more than one entry in the **AE Titles** section, select the relevant AE title.
4. Click **DICOM Verify**. The **Server DICOM Verify** window appears confirming whether the connection is working.



5. Click **OK** to close the window.

4.2.8 Add New Device Window Elements

The following table lists the elements that appear in the New Device window. The elements that are common to a number of devices are listed first.

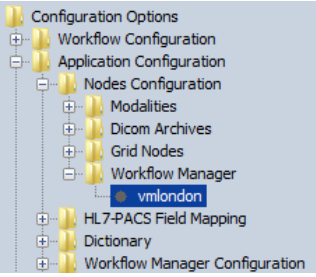
Element	Type	Description
Common Elements		
Node Name	Text box	The name of the device. This is the name that appears in the navigation tree in the left pane of the System Configuration tool.
IP	Text box	The IP address of the device.
Site ID	Text box	The site ID that is used to identify studies from this device. Relevant only when there is more than one site within the network.
Issuer	Text box	The issuer assigning the patient ID from this device.

Element	Type	Description
Node Info	Button	Click to view information about the node, such as the IP address and port. In the Device Information window that appears, you can view information about the current node, or you can scroll through the window to view information on all nodes configured in the network.
Access Control	Button	Click to assign or remove restrictions for accessing data from this device. For example, when there is more than one site in a network, you can restrict data access according to the site ID, so that only individual sites will see data relating to that site. For more information on using data restrictions, see Section 3.7 Assigning Restrictions to Users and Groups.
Name	Text box	The name of the device.
AE	Text box	The unique name, which identifies the application entity instance to other DICOM entities on the network. The AE title is case sensitive and has a maximum of 16 characters.
Port	Text box	The port used by the application entity instance for DICOM communication.
Queryable	Text box	Indicates whether DICOM queries can be sent to the device.
Storable	Text box	Indicates whether DICOM images can be stored on the device. For example, a previous mammography exam for a patient can be sent to the modality so the technician can view it before performing the current exam.
Device Type	Text box	The device type. This value is populated automatically.
Add	Button	Click to add the AE title, port and other details for the device.
Delete	Button	Click to delete the device.
DICOM Verify	Button	Click to verify DICOM connectivity to the device.
The AE Titles configured above are Virtual AEs	Check box	For future use. Indicates whether the AE title instances are virtual. That is, they are additional AE titles that can be used to connect to this device.
Outgoing DICOM AE	Drop-down list	The AE-title used when sending outgoing DICOM messages to this device. Possible values are: • Source AE (default) • Default mask – This is the virtual AE.
Storage Commitment Policy	Drop-down list	Specifies how the storage commitment response is sent. Possible values are: • Same association (default) • New association • Not allowed

Element	Type	Description
Transfer Syntax Policy	Drop-down list	Specifies the DICOM transfer syntax that is offered and accepted by the device. Possible values are: • Standard DICOM (default) – Includes Explicit Big, Explicit Little, and Implicit Little syntax • Implicit Little – Recommended when troubleshooting DICOM connectivity problems • Private – Recommended for communication between Carestream PACS components • Custom – Transfer syntaxes are manually configured in the Central Configuration • Adaptive – Use custom transfer syntaxes for SOP classes that need to be transferred. Recommended when image compression should not be affected. In addition, if pixel data is compressed, you can select the compression algorithm used: • JPEG Lossless • JPEG Lossy • JPEG Lossy/ Lossless 2000 • JPEG Lossless 2000 • JPEG Lossy Baseline • JPEG Lossy Extended • JPEG Lossless 1st Order Predictions • JPEG Lossless PR14 • RLE Lossless
Advanced SOP Classes Settings	Button	Click to open the Advanced SOP Classes Settings window in which you define the known storage SOP classes that are excluded from the negotiation phase of an association and the SOP classes that are added to an association. See Section 4.3.5.3 Configuring Advanced SOP Classes Settings for more information.
Printer Elements		
Select printer kind	Drop-down list	Specifies the manufacturer and model of the printer to be added.
Set as Default Printer	Check box	Indicates whether the printer is the default printer.
Printer configuration	Text box	Optional printer configuration parameters set in the DICOM print request (tag 2010,0150 – Configuration Information). Used when the printer vendor supports implementation-specific print parameters or one or more configuration data values encoded as characters.
Reporting and Remote Web Portal Elements		
Supports Grid	Check box	Indicates whether the Speech Server is part of a grid network.

4.3 Updating the Workflow Manager Node Configuration

The Workflow Manager is highly configurable and can be expanded to accommodate growing storage and archiving needs. To view the current configuration, select the Workflow Manager node in the left pane of the System Configuration tool.

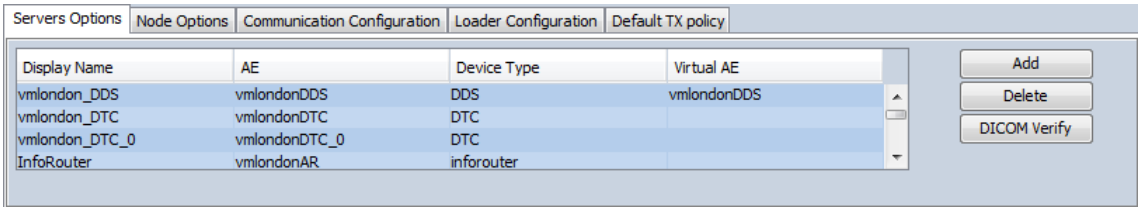


From here, you can do the following:

- View the processes configured for this Workflow Manager
- Specify allowed and forbidden hosts
- View the communication configuration
- Update the loader configuration
- Update the default transfer syntax4.3.2 policy

4.3.1 Viewing the AE Configuration

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration** and select the Workflow Manager. The **DICOM** tab appears in the right pane, open on the **Servers Options** tab.



2. You can view the list of processes configured for the Workflow Manager and you can verify the connection to the server, if required. See Section 4.2.7 Verifying the DICOM Connection for more information.

   Note: When you select a process, the Server Options tab expands to include additional elements.

   See Section 4.3.6 DICOM Tab Elements for more information about each of the elements in the **Servers Options** tab.

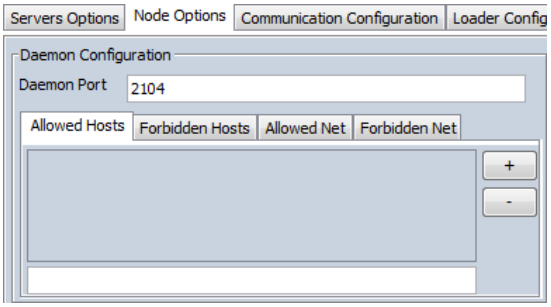
   Note: Consult with Carestream Professional Services personnel before making any changes to the Workflow Manager server configuration.

4.3.2 Specifying Allowed and Forbidden Hosts

You can restrict access to the Workflow Manager based on the host address of the source machine.

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration** and select the Workflow Manager. The **DICOM** tab appears in the right pane.

2. Select the **Node Options** tab.



3. Use the following tabs to enter the allowed or forbidden host addresses from which the Workflow Manager can receive DICOM images:

• Allowed Hosts • Forbidden Hosts	Type the exact IP address.
• Allowed Net • Forbidden Net	Type the net address. For example, type 192.168, to allow or restrict devices with an IP address that belongs to the 192.168 net.

4. Click +

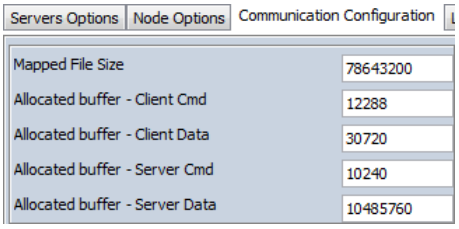
5. Repeat steps 3–4 for additional host addresses, as required.

   See Section 4.3.6 DICOM Tab Elements for more information about each of the elements in the **Node Options** tab.

4.3.3 Viewing the Communication Configuration

IMPORTANT: The communication configuration parameters are set by Carestream Professional Services personnel and are for Carestream use only.

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration** and select the Workflow Manager. The **DICOM** tab appears in the right pane.
2. Select the **Communication Configuration** tab, which shows the mapped file size and allocated buffers.

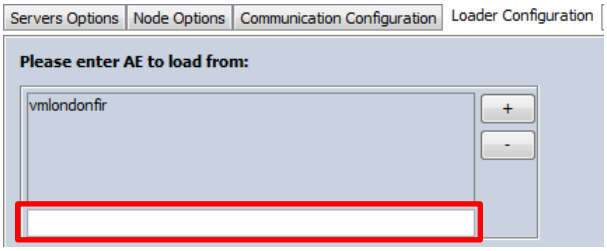


   See Section 4.3.6 DICOM Tab Elements for more information about each of the elements in the **Communication Configuration** tab.

4.3.4 Updating the Loader Configuration

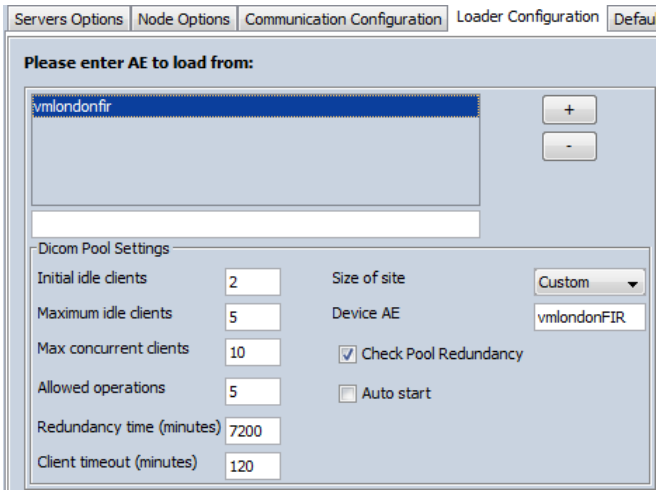
1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration** and select the Workflow Manager. The **DICOM** tab appears in the right pane.

2. Select the **Loader Configuration** tab.



3. In the box, type the AE title from which to load and click +.

   The **Loader Configuration** tab expands to include the **DICOM Pool Settings**.



4. Enter the appropriate values in the **DICOM Pool Settings** boxes.

   See Section 4.3.6 DICOM Tab Elements for more information about each of the elements in the **Loader Configuration** tab.

4.3.5 Updating the Default Transfer Syntax Policy

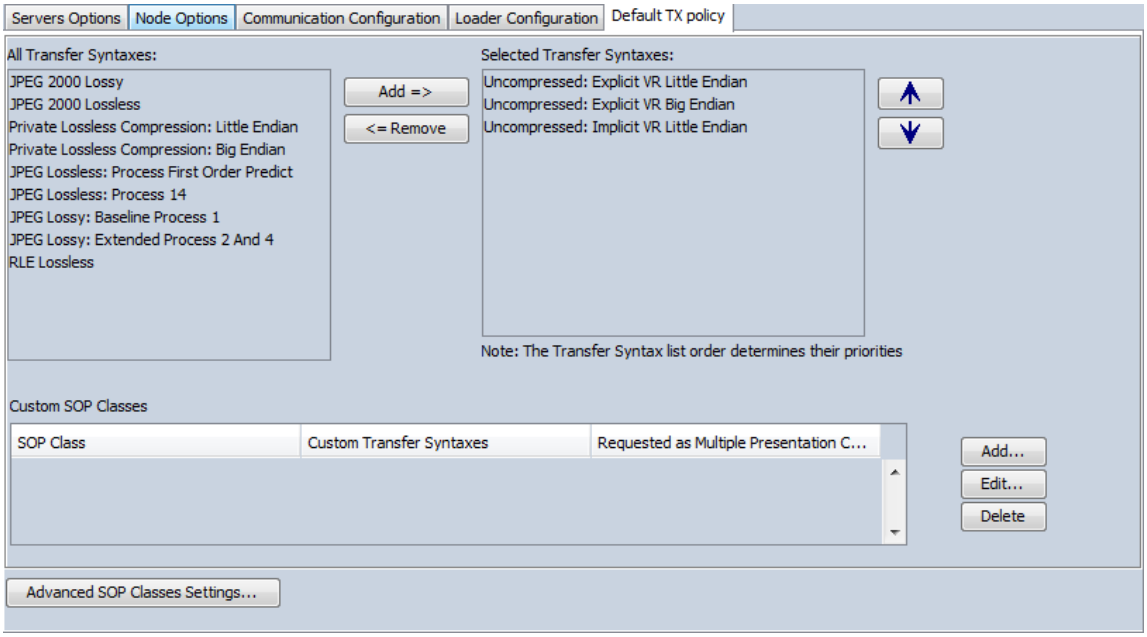
The transfer syntax policy specifies the DICOM transfer syntax that is offered and accepted by a device.

You can update the Workflow Manager's default transfer syntax policy for non-customized SOP classes. In addition, you can customize the SOP classes, or exclude or add SOP classes from the association.

4.3.5.1 Selecting the Transfer Syntax

1. In the left pane of the System Configuration tool, navigate to **Nodes Configuration** and select the Workflow Manager. The **DICOM** tab appears in the right pane.

2. Select the **Default TX Policy** tab.

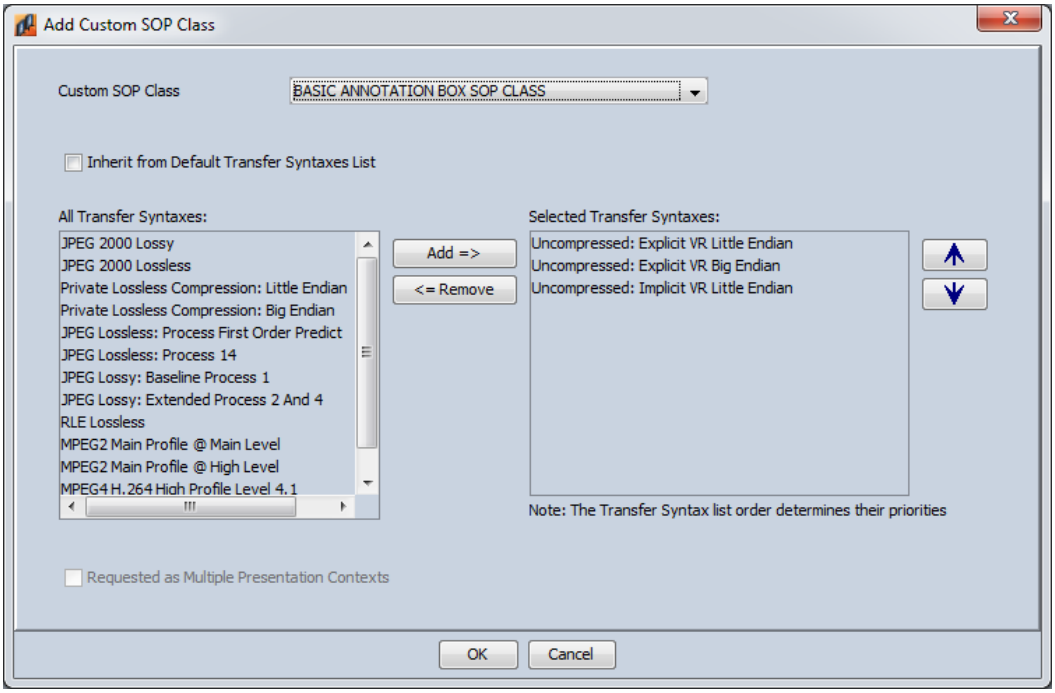


3. From the **All Transfer Syntaxes** list, select the required transfer syntaxes, and click **Add**. The selected transfer syntax appears in the **Selected Transfer Syntaxes** list.
4. Use the  and  buttons to change the order of the selected transfer syntaxes.

   See Section 4.3.6 DICOM Tab Elements for more information about each of the elements in the **Default TX Policy** tab.

4.3.5.2 Customizing an SOP Class

1. In the Default TX Policy tab, click **Add**. The **Add Custom SOP Class** window opens.

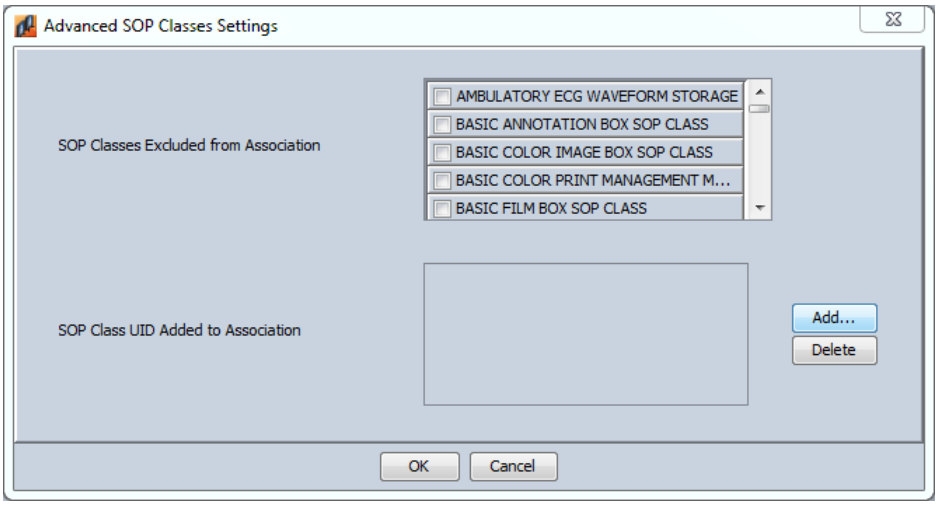


2. Select the SOP class that you would like to customize from the **Custom SOP Class** drop-down list.
3. Select the **Inherit from Default Transfer Syntaxes List** check box to use the default transfer syntaxes defined in the **Default TX Policy** tab for this SOP class. This is useful if you want to configure multiple presentation contexts.
4. If you do not select the **Inherit from Default Transfer Syntaxes List** check box, then you need to select the transfer syntaxes that are relevant for this SOP class and click the **Add** button to move them to the Selected Transfer Syntaxes list.
5. Use the  and  buttons to change the order of the selected transfer syntaxes.
6. Select the **Requested as Multiple Presentation Contexts** check box to use multiple presentation contexts when requesting the specific SOP class. This option is relevant only when acting as the client side.
7. Click **OK** to close the window.

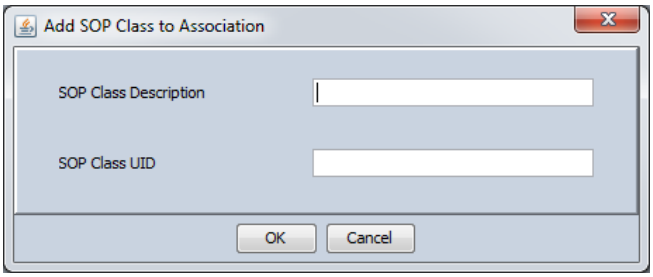
4.3.5.3 Configuring Advanced SOP Classes Settings

You can configure known storage SOP classes that are excluded from the negotiation phase of an association and the SOP classes that are added to an association. These settings apply to all DICOM peers that are not configured as a device in the system configuration.

1. Click the **Advanced SOP Classes** button to open the **Advanced SOP Classes Settings** window.



2. In the **SOP Classes Excluded from Association** list, select any non-relevant SOP classes that can be excluded from the association.
3. To add additional SOP classes to an association, click the **Add** button. The **Add SOP Class to Association** window opens.



4. Enter the SOP Class Description and SOP Class UID in the relevant fields and click **OK**.
5. In the **Advanced SOP Classes Settings** window, click **OK** to close the window.

4.3.6 DICOM Tab Elements

The following table lists the elements that appear in the DICOM tab.

Element	Type	Description
Common Elements		
Node Name	Text box	The name of the device. This is the name that appears in the navigation tree in the left pane of the System Configuration tool.
IP	Text box	The IP address of the device.
Site ID	Text box	The site ID that is used to identify studies from this device. Relevant only when there is more than one site within the network.
Issuer	Text box	The issuer assigning the patient ID from this device.
Users Domain	Text box	The domain name assigned to users defined locally on this server (not via LDAP) that is used to differentiate between these users and users from other servers in the grid.
Supports Grid	Check box	Indicates whether the Workflow Manager is part of a grid network.
Node Info	Button	Click to view information about the node, such as the IP address and port. In the Device Information window that appears, you can view information about the current node, or you can scroll through the window to view information on all nodes configured in the network.
Access Control	Button	Click to assign or remove restrictions for accessing data from this device. For example, when there is more than one site in a network, you can restrict data access according to the site ID, so that only individual sites will see data relating to that site. For more information on using data restrictions, see Section 3.7 Assigning Restrictions to Users and Groups.
Servers Options Tab		
Display Name	Column	When the DX check box is selected, this is the name that appears in the Vue PACS client Archive Explorer.
AE	Column	The unique name, which identifies the application entity instance to other DICOM entities on the network. The AE title is case sensitive and has a maximum of 16 characters.
Device Type	Column	The role of the AE on the server.
Virtual AE	Column	Indicates whether the AE instance is a virtual AE. This are additional AE titles that are associated with this application.
Add	Button	Click to add an optional service to the Workflow Manager.
Delete	Button	Click to delete the service.
DICOM Verify	Button	Click to verify DICOM connectivity to the service.
Activate Backup Rule	Check box	Relevant for services where the device type is DISK. Indicates whether studies are backed up by the Info Router.

Element	Type	Description
Automatically mark studies as “backed up”	Check box	Relevant for services where the device type is DISK. Indicates whether the Info Router marks the copied studies as backed up after a configurable amount of time.
Port	Text box	The port used by the application entity instance for DICOM communication.
Parallel Associations	Text box	The number of associations to open when storing images to this application entity. Possible values are from 1 to 4.
Database Path	Text box	Relevant for services where the device type is FOLDER or DISK. This is the directory where the images are saved.
Timeout (Minutes)	Text box	The maximum time to wait for a socket event.
Enable Dicom to conn interface	Check box	Relevant for services where the device type is DTC. Enables the DICOM to Conn service.
Global Worklist AE Title	Text box	The AE title of the remote grid node that the DTC service works with.
Supports Store	Check box	Indicates whether the Vue PACS client can store images to this application entity.
Supports Delete	Check box	Indicates whether the Vue PACS client can delete images from this application entity.
Supports Query	Check box	Indicates whether the Vue PACS client can retrieve images from this application entity.
Supports DX Store Presentation State	Check box	Indicates whether the Vue PACS client can store the presentation state to this application entity.
Invoke Filter	Check box	Indicates whether the filter is invoked automatically in the Vue PACS client.
Classified	Check box	Indicates whether the patient name in stored studies is changed to initials.
Uncompressed	Check box	Indicates whether newly-stored DICOM images are not compressed.
Read only	Check box	Indicates whether the folder is read-only.
Presentation State C-Move Policy	Drop-down list	Determines what is done with presentation states when they are copied to this application entity. Possible values are: • Standard (as is) • Move with referenced images • Apply presentation state • Ignore presentation state
Multiple Reports C-Move Policy	Drop-down list	Determines what is done with studies when they are copied to this application entity. Possible values are: • Move only requested study • Include referenced study (images) • Include all SRs and referenced study

Element	Type	Description
Key Object Selection C-Move Policy	Drop-down list	Determines what is done with key object selections when they are copied to this application entity. Possible values are: • Standard (as is) • Move with referenced images • Apply KOS • Ignore KOS
Create Folders in DX	Check box	Indicates whether a folder for the DICOM folder is created in the Vue PACS client.
Search	Text box	The name of the Search folder as it appears in the Vue PACS client.
All Studies	Text box	The name of the All Studies folder as it appears in the Vue PACS client.
All Patients	Text box	The name of the All Patients folder as it appears in the Vue PACS client.
Auto Delete	Check box	Indicates whether to automatically delete studies from the DICOM folder when the studies pass the threshold number of days allowed or when the folder size exceeds the allowed amount.
Days to keep	Text box	The maximum number of days to keep studies in the DICOM folder.
Delete up to (MB)	Text box	The maximum size of the DICOM folder.
Node Options Tab		
Daemon Port	Text box	The port used by the application entity instance for DICOM communication.
Allowed Hosts	Tab	The IP addresses from which the Workflow Manager can receive DICOM images.
Forbidden Hosts	Tab	The IP addresses that are restricted for the Workflow Manager and from which no DICOM images are received.
Allowed Net	Tab	The allowed net addresses from which the Workflow Manager can receive DICOM images.
Forbidden Net	Tab	The net addresses that are restricted for the Workflow Manager and from which no DICOM images are received.
Plus	Button	Click to add allowed or forbidden host addresses.
Minus	Button	Click to remove allowed or forbidden host addresses.
Communication Configuration Tab		
Mapped File Size	Text box	For Carestream use only.
Allocated buffer – Client Cmd	Text box	For Carestream use only.
Allocated buffer – Client Data	Text box	For Carestream use only.
Allocated buffer – Server Cmd	Text box	For Carestream use only.
Allocated buffer – Server Data	Text box	For Carestream use only.

Element	Type	Description
Loader Configuration Tab		
AE to load from	Text box	For Carestream use only.
Plus	Button	Click to add AE titles to load from.
Minus	Button	Click to remove AE titles to load from.
Default TX Policy		
All Transfer Syntaxes	List	The available transfer syntaxes.
Selected Transfer Syntaxes	List	The selected transfer syntaxes. You set the order of priority using the up and down arrows.
Add	Button	Click to move the selected transfer syntax to the Selected Transfer Syntaxes list.
Remove	Button	Click to remove the selected transfer syntax from the Selected Transfer Syntaxes list.
Move up	Button	Click to move the selected transfer syntax up the list. The list order defines the priority of the transfer syntax.
Move down	Button	Click to move the selected transfer syntax down the list. The list order defines the priority of the transfer syntax.
SOP Class	Column	The SOP class that is customized.
Custom Transfer Syntaxes	Column	The supported transfer syntaxes of the customized SOP class. The order defines the priority of the transfer syntax.
Requested as Multiple Presentation Context	Column	Not applicable for the default DICOM configuration.
Add	Button	Click to open the Add Custom SOP Class window, in which you select the SOP class to customize and the supported transfer syntaxes. See Section 4.3.5.2 Customizing an SOP Class for more information.
Edit	Button	Click to edit a customized SOP class.
Delete	Button	Click to remove a customized SOP class.
Advanced SOP Classes Settings	Button	Click to open the Advanced SOP Classes Settings window, in which you can exclude irrelevant SOP classes from the association or add new SOP Classes that are currently not supported: See Section 4.4.5.3 Configuring Advanced SOP Classes Settings for more information.

4.4 Configuring the Workflow Manager

The Workflow Manager provides workflow management, distribution and archive capabilities that automate workflow and data management. These features create a convenient and efficient working environment for users and administrators.

The Workflow Manager maintains the single site or global enterprise database, manages the DICOM and non-DICOM online storage, manages multi-tier storage, coordinates near-line and offline storage, controls RIS connectivity and synchronization, reconciles patient information, initiates pre-fetches, and automatically routes images and information quickly and efficiently to any location throughout the enterprise.

You can use the System Configuration tool to configure the following Workflow Manager features:

- DICOM parsing rules
- Study grouping rules
- Pre-fetch rules
- Push to client rules
- Icon settings
- Compression settings
- Init values

4.4.1 Configuring DICOM Parsing Rules

You use DICOM parsing rules to set an initial value for a tag or to map specific DICOM tags to different or multiple tags. For example, if a modality uses a single field for two values, the DICOM parsing rules can be configured to break down this information into two distinct DICOM tags.

You can configure the following types of parsing rules:

- **Pre-Defined** – Use to set an initial value for a tag. You can do this in one of the following ways:
  - Set the value in a tag to a fixed value. For example, add the site ID to all incoming studies.
  - Remove a tag completely.
  - Clear the value of a tag.
- **Basic** – Use to copy values from one tag to another or to split the value in a tag into separate target tags.

  For example, for cardiac CT images, you can define a parsing rule to copy the last two characters (number) from the SERIES_DESCRIPTION tag to TAMAR_IMAGE_PHASE.
- **Advanced** – Use to copy values from one tag to another using an advanced pattern.

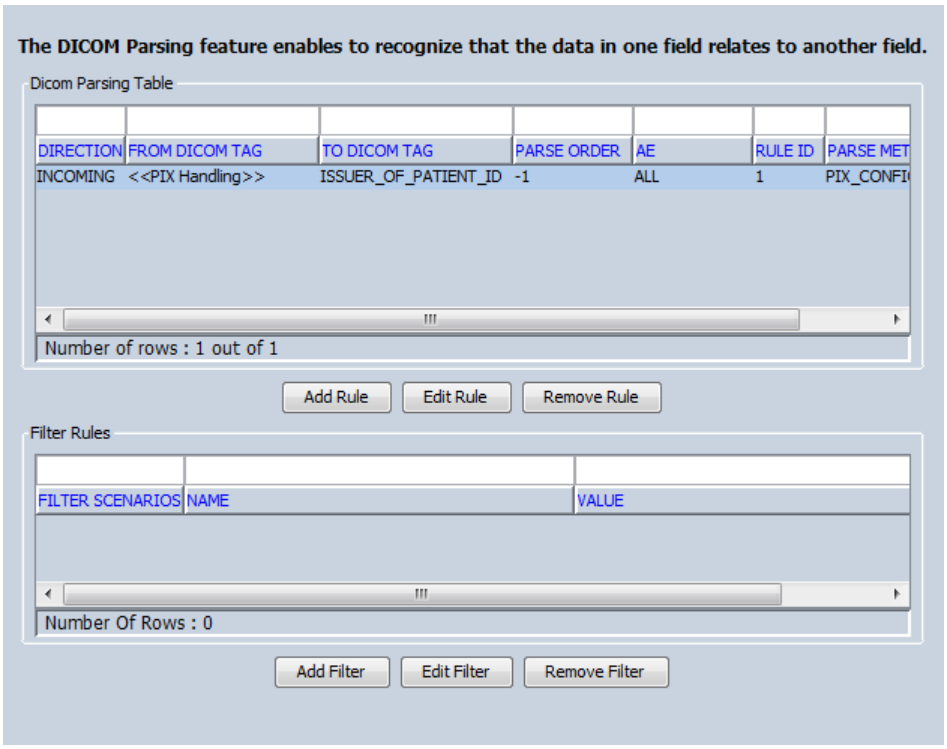
  For example, if the patient ID in the source tag includes leading zeros, which are not required in the target tag, you can define a parsing rule to remove the leading zeros.
- **Conversion Table** – Use to convert specific values in a source tag to another value based on value mappings in a table.

  For example, in a multi-site environment, you can set the issuer target tag according to the site ID source tag.

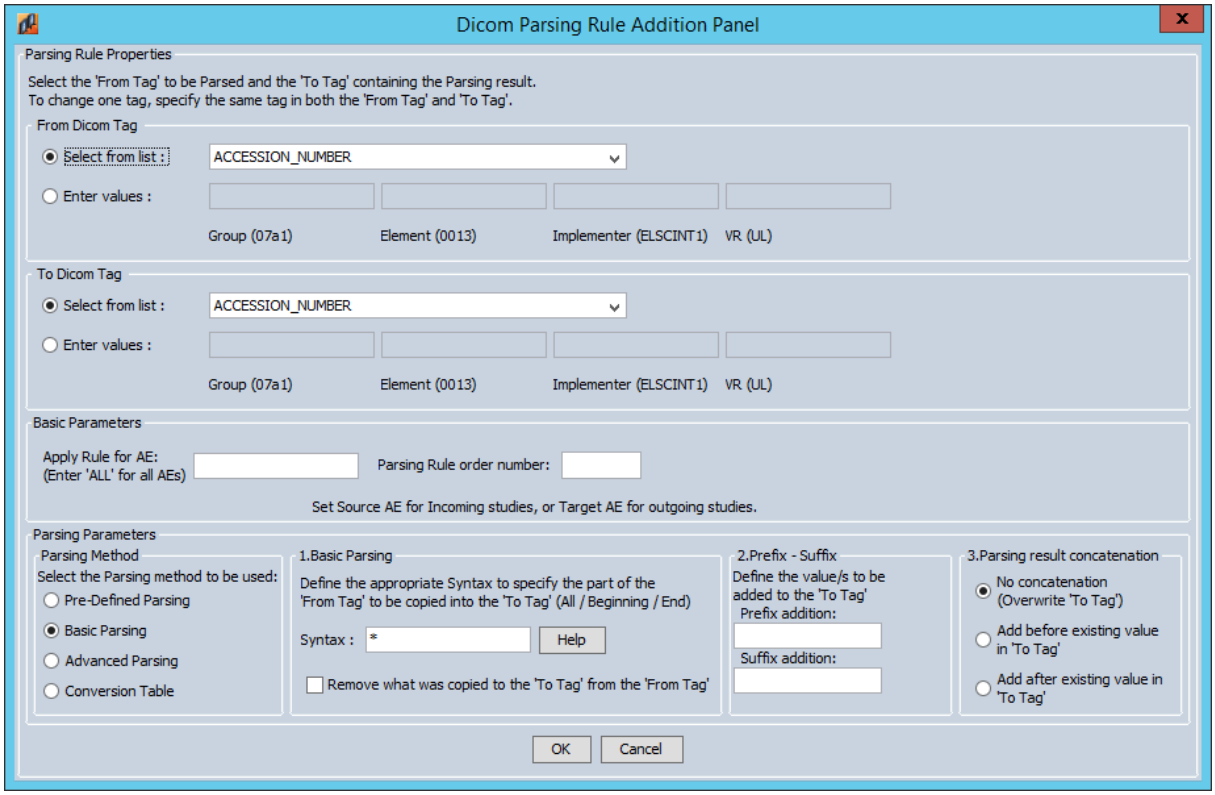
Note: Carestream recommends that you consult with Carestream Professional Services personnel before adding or modifying DICOM parsing rules.

4.4.1.1 Adding a DICOM Parsing Rule

1. In the left pane of the System Configuration tool, navigate to **Application Configuration > Workflow Manager Configuration > DICOM Parsing**. The rule display area appears in the right pane containing two sections:
   - The **DICOM Parsing Table** section lists the DICOM parsing rules.
   - The **Filter Rules** section lists the filter rules that apply to each of the DICOM parsing rules above.



2. Click **Add Rule**. The **DICOM Parsing Rule Addition Panel** window appears.



3. In the **Parsing Parameters** section, select the parsing method to use.
    - **Pre-Defined Parsing** – Use to set an initial value for a tag. In this case, the From DICOM Tag is not required.
    - **Basic Parsing** – Use to copy values from one tag to another.
    - **Advanced Parsing** – Use to copy values from one tag to another using an advanced pattern.
    - **Conversion Table** – Use to convert specific values in the FROM DICOM Tag to another value based on value mappings in a table.
4. In the **From DICOM Tag** section, select the tag that you wish to map *from* in the **Select from list** drop-down (not required for pre-defined parsing).

    OR

    Enter the values in the **Group**, **Element**, **Implementer**, and **VR** text boxes.
5. In the **To DICOM Tag** section, select the tag that you wish to map *to* in the **Select from list** drop-down.

    OR

    Enter the values in the **Group**, **Element**, **Implementer**, and **VR** text boxes.
6. To define a parsing rule for a specific AE, in the **Basic Parameters** section, type the AE title in the **Apply Rule for AE** text box. Otherwise, type **ALL** for all AEs.

    Note: The AE title is case sensitive and has a maximum of 16 characters.
7. In the **Parsing Rule order number** text box, type a number, which defines the order of the parsing rule in relation to other parsing rules.
8. Now you define the parsing parameters that are relevant for the parsing method that you chose in step 3.
    a. If you selected pre-defined parsing, in the **Pre-Defined Parsing** section, select one of the following options:
        - **To DICOM Tag value** – Select this option to set the value in the **To DICOM Tag** to a fixed value. Type the value in the text box.
        - **Remove To DICOM Tag** – Select this option to remove the **To DICOM Tag**.
        - **Clear To DICOM Tag** – Select this option to clear the value of the **To DICOM Tag**.

    b. If you selected basic parsing, in the **Basic Parsing** section:

    i. Type the syntax that specifies the part of the source tag to copy to the target tag. The syntax uses regular expressions, such as ***** and **/.***. Click **Help** for a detailed explanation and examples.

    ii. Select the **Remove what was copied to the To Tag from the From Tag** check box, if required.

    For example, if the **BODY_PART_EXAMINED** tag contains the body part and the patient ID, select this tag in the **From DICOM Tag** section.
    Then select the **PATIENT_ID** tag in the **To DICOM Tag** section.
    In the **Syntax** text box, type **/.*** and select the **Remove what was copied to the To Tag from the From Tag** check box.
    This results in two tags: the **BODY_PART_EXAMINED** tag and the **PATIENT_ID** tag.

c. If you selected advanced parsing, in the **Advanced Parsing** section:

i. Type the syntax for the pattern to search for in the source tag. The pattern uses regular expressions with special characters, such as *****, **^** and **$**. Click **Help** for a detailed explanation and examples.

ii. Select one of the following options:

- **Copy Pattern** – Select this option to copy the pattern to the target tag.
- **Replace Pattern with** – Select this option to replace the pattern in the target tag with the replacement text (or no text).

iii. Select one of the following options:

- **First occurrence** – Select this option to copy only the first occurrence of the pattern to the target tag.
- **All occurrences** – Select this option to replace all occurrences of the pattern in the target tag with the replacement text (or no text).

iv. Select the Remove what was copied to the To Tag from the From Tag check box, if required.

For example, if the patient ID in the source tag includes leading zeros, which are not required in the target tag, select **PATIENT_ID** in both the **From DICOM Tag** and **To DICOM Tag** sections.
In the **Pattern** text box, type **^0*** and select the **Replace Pattern with** option, but leave it empty.
The leading zeros will be removed from the target tag.

d. If you selected to convert specific values, click **Edit Conversion Table**. In the window that opens, click the **Add Data** button to add the values that you want to replace and the values that you want to replace them with.

For example, if you have a multi-site environment, if the site ID in the source tag is 1 then you can set the Issuer target tag to x; if the site ID is 2 then you can set the Issuer target tag to y.

For more information on using conversion tables, see Section 4.5.1.2 Using DICOM Parsing Conversion Tables.

9. To add a prefix or suffix to the target tag, in the **Prefix - Suffix** section, enter the value to be added in the relevant text box.
10. To concatenate the parsing results (not relevant for pre-defined parsing), in the **Parsing result concatenation** section, select one of the following values:
    a. No concatenation (Overwrite To Tag)
    b. Add before existing value in To Tag
    c. Add after existing value in To Tag

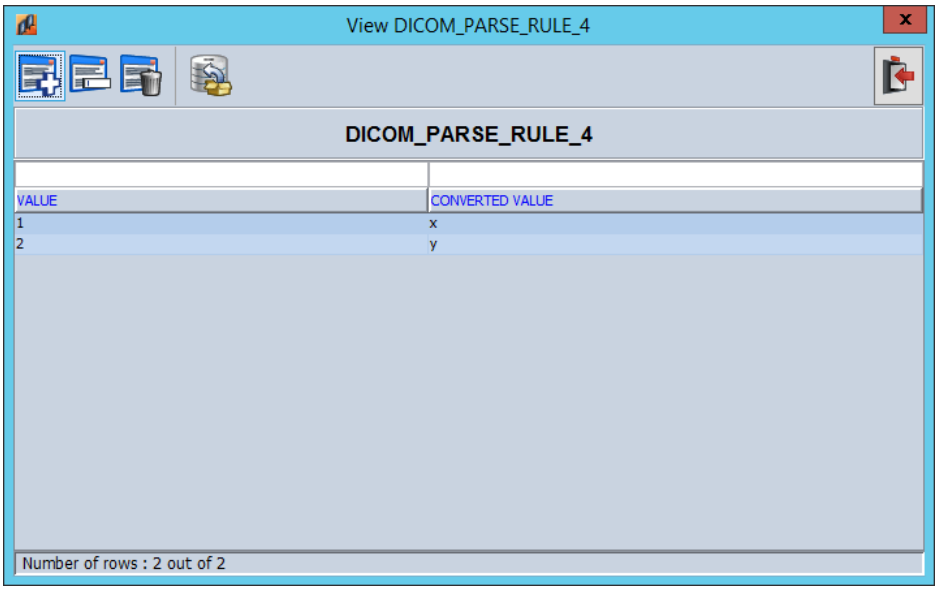
    Add a separation string, if required
11. Click **OK** to return to the rule display area.

4.4.1.2 Using DICOM Parsing Conversion Tables

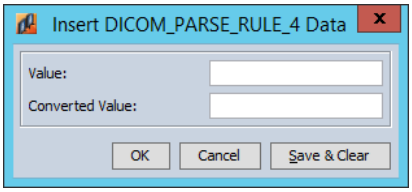
You can create a conversion table to convert specific values in DICOM parsing rules, or you can import a file that contains values separated by a delimiter.

To create a conversion table:

1. In the **DICOM Parsing Rule Addition Panel** window, in the **Parsing Method** section, select **Conversion Table**.
2. Click **Edit Conversion Table**. The **View DICOM_PARSE_RULE** window opens.



3. Click the **Add Data** button. The **Insert DICOM_PARSE_RULE Data** window opens.

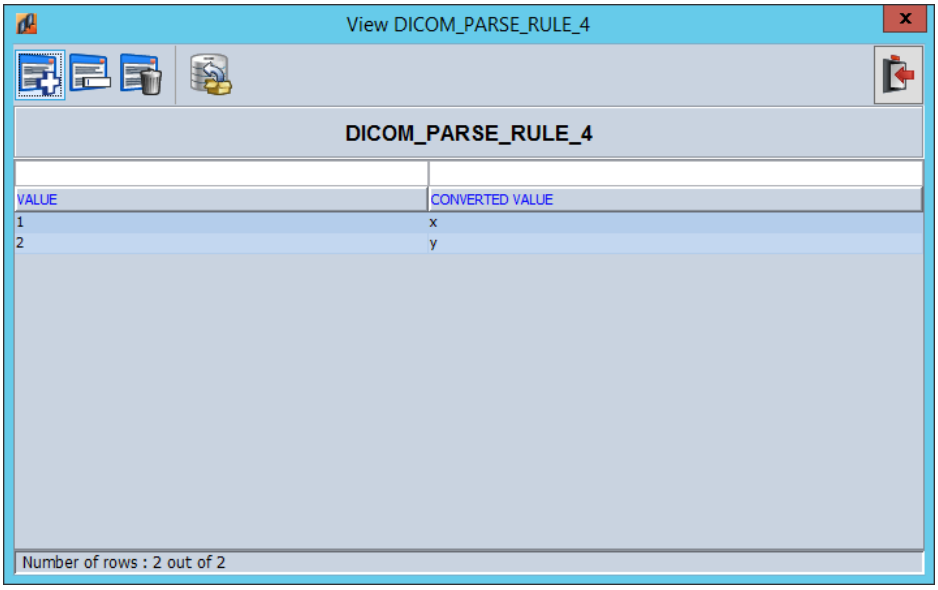


4. Type the value you want to replace and the converted value and click **OK**.
5. Repeat steps 3 and 4 to add more values.
6. Click the **Exit** button to close the **View DICOM_PARSE_RULE** window and return to the **DICOM Parsing Rule Addition Panel** window.

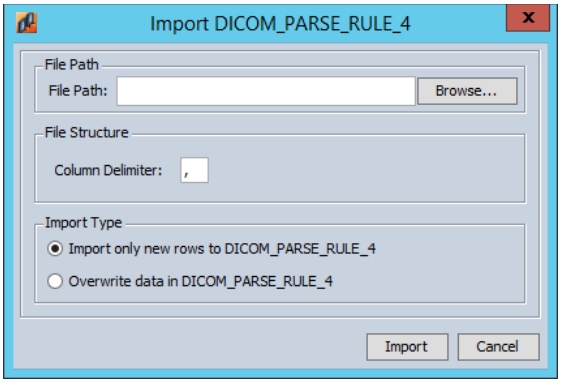
To import a conversion file:

1. In the **DICOM Parsing Rule Addition Panel** window, in the **Parsing Method** section, select **Conversion Table**.

2. Click **Edit Conversion Table**. The **View DICOM_PARSE_RULE** window opens.



3. Click the **Import DICOM_PARSE_RULE Data** button. The **Insert DICOM_PARSE_RULE Data** window opens.



4. Type the location of the conversion file in the **File Path** box or click **Browse** to find the location.
5. In the **Column Delimiter** box, type the delimiter used to separate the columns in the conversion file.
6. In the **Import Type** section, select whether to import new rows or overwrite data in the **DICOM_PARSE_RULE** table.
7. Click **Import** to import the conversion table.
8. When the conversion table is imported successfully, click **OK** in the message that appears to return to the **View DICOM_PARSE_RULE** window.
9. Click the **Exit** button to close the **View DICOM_PARSE_RULE** window and return to the **DICOM Parsing Rule Addition Panel** window.

4.4.1.3 Editing a DICOM Parsing Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > DICOM Parsing**.
2. In the rule display area in the right pane, select the rule and click **Edit Rule**. The **DICOM Parsing Rule Addition Panel** window appears.

3. Edit the rule. See Section 4.4.1.3 Editing a DICOM Parsing Rule for details.

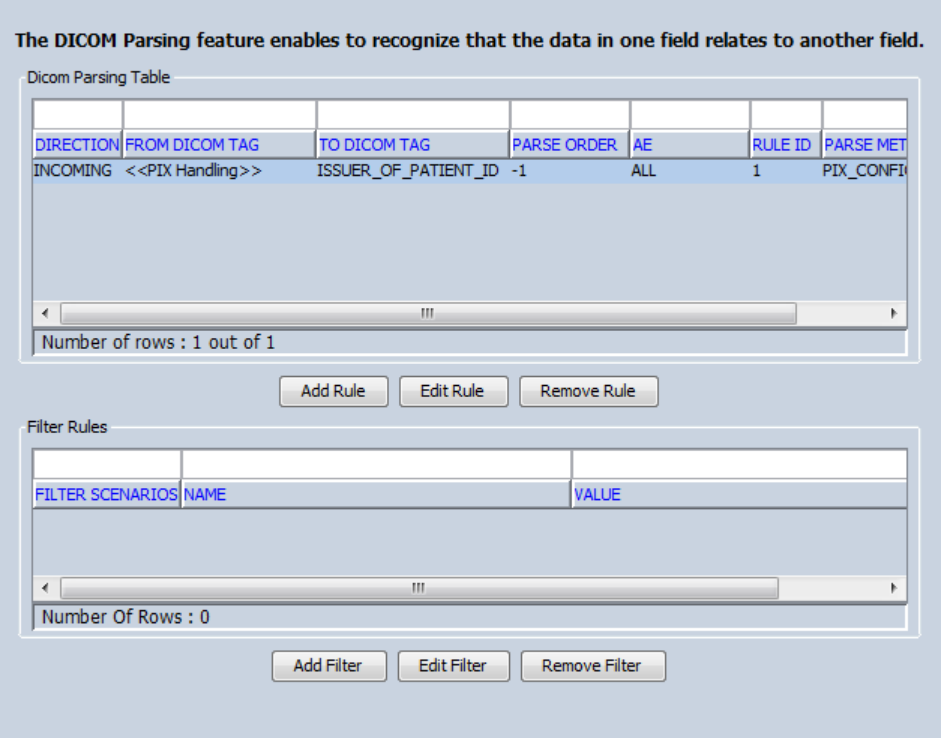
4.4.1.4 Removing a DICOM Parsing Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > DICOM Parsing**.
2. In the rule display area in the right pane, select the rule and click **Remove Rule**.
3. In the confirmation message that appears, click **Yes**.

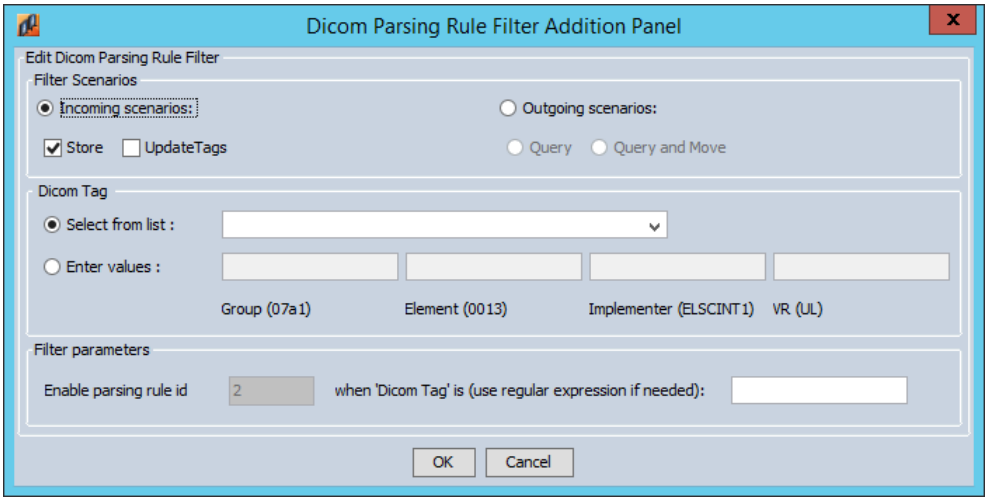
   The rule is removed from the rule display area.

4.4.1.5 Adding a Filter for a DICOM Parsing Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > DICOM Parsing**. The rule display area appears in the right pane. It contains two sections: the **DICOM Parsing Table** section lists the DICOM parsing rules; the **Filter Rules** section lists the filter rules that apply to each of the DICOM parsing rules above.



2. Click **Add Filter**. The **DICOM Parsing Rule Filter Addition Panel** window appears.



3. In the **Filter Scenarios** section, select one of the following options:
   - **Incoming scenarios** (default) – Use this option to parse incoming data. Then select the **Store** or **Update Tags** check box, or both.
   - **Outgoing scenarios** – Use this option to parse outgoing data. Then select the **Query** or **Query and Move** options. This scenario is less common but can be used, for example, to remove tags that are not handled by the target system.

4.4.1.6 Editing a Filter for a DICOM Parsing Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > DICOM Parsing**.
2. In the rule display area in the right pane, select the rule and click **Edit Rule**. The **DICOM Parsing Rule Addition Panel** window appears.
3. Edit the rule. See Section 4.4.2.1 Adding a Study Grouping Rule for details.

4.4.1.7 Removing a Filter for a DICOM Parsing Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > DICOM Parsing**.
2. In the rule display area in the right pane, select the rule and click **Remove Rule**.
3. In the confirmation message that appears, click **Yes**.

   The rule is removed from the rule display area.

4.4.2 Configuring Study Grouping Rules

You use study grouping rules to group studies together. For example, if an incoming study has the same accession number and patient ID as an existing study, you can group them together into one study with a single study instance ID.

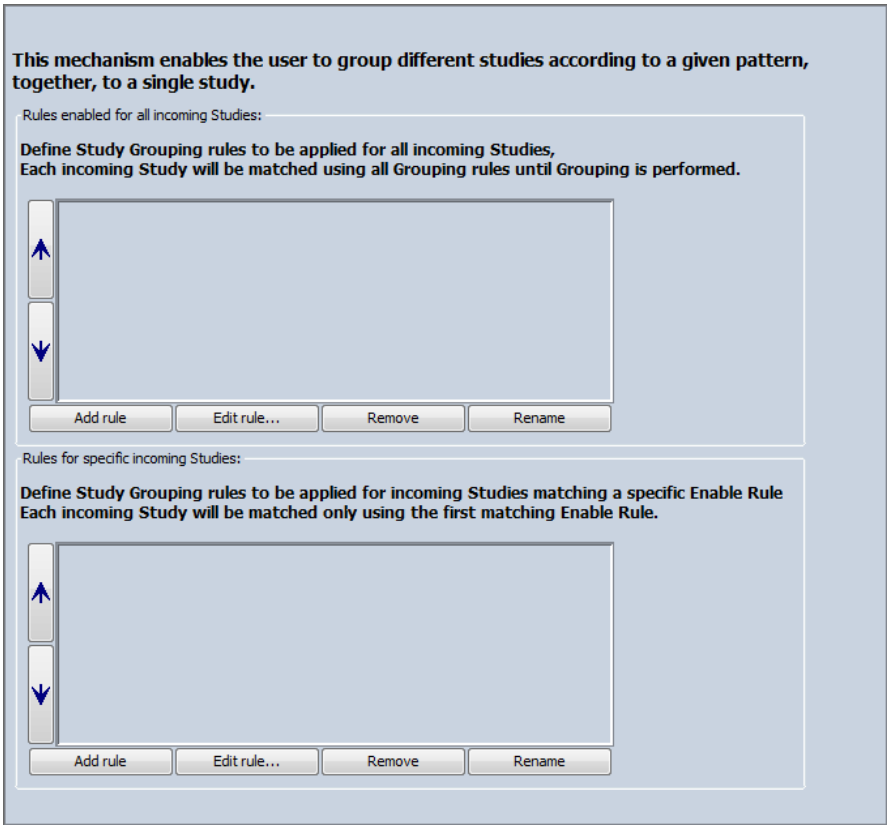
The study grouping mechanism uses compare rules to compare one study with another. These compare rules can be applied to all incoming studies, or to specific studies only, in which case filter rules are used to decide which of the studies are compared.

When you configure study grouping rules, the information is reflected in the Central Configuration in the following location:

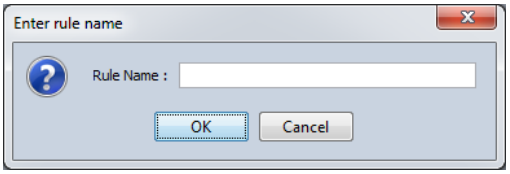
```
imaginet\system\applications\medistore\didb\study_matching_system_rules
```

4.4.2.1 Adding a Study Grouping Rule

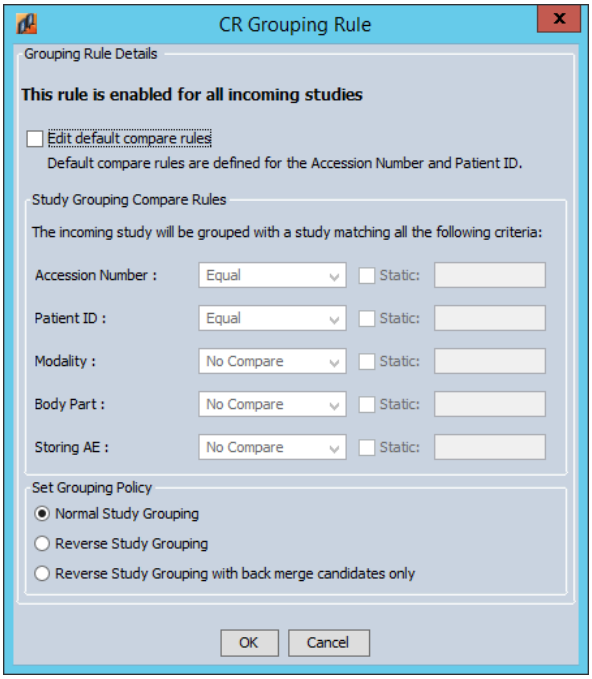
1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Study Grouping**. The rule display area appears in the right pane containing two sections: the upper section is for rules that apply to all incoming studies; the lower section is for rules that apply to specific studies only.



2. To define rules that apply to all incoming studies, click **Add rule** in the upper section. The **Enter Rule Name** window appears.



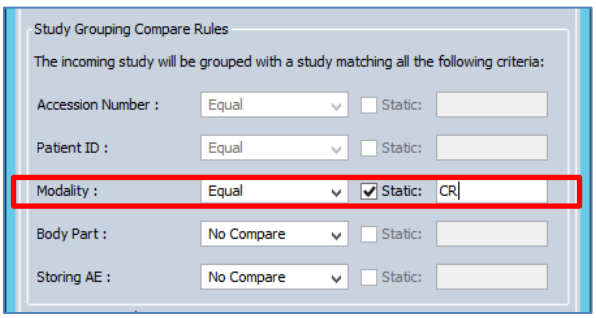
3. Type the rule name and click **OK**. The **Grouping Rule Details** window appears.



4. By default, the accession number (which identifies the order for the study) and the patient ID are used to compare studies. To add criteria, select the **Edit default compare rules** check box. The additional criteria are enabled for selection.
5. Select the additional criteria operator from the relevant drop-down list. For example, to compare studies from the same modality, from the **Modality** drop-down list, select **Equal**.

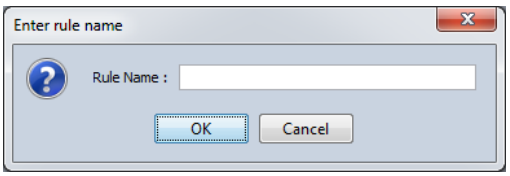
Note: For the Contains operator, you can use a regular expression. For example, if Modality contains *SR*, the mechanism will match CT-SR and MR-SR modalities.

6. To use a fixed value for the additional criteria, select the **Static** checkbox and type a value in the text box. For example, to compare only CR studies, type **CR** in the text box.

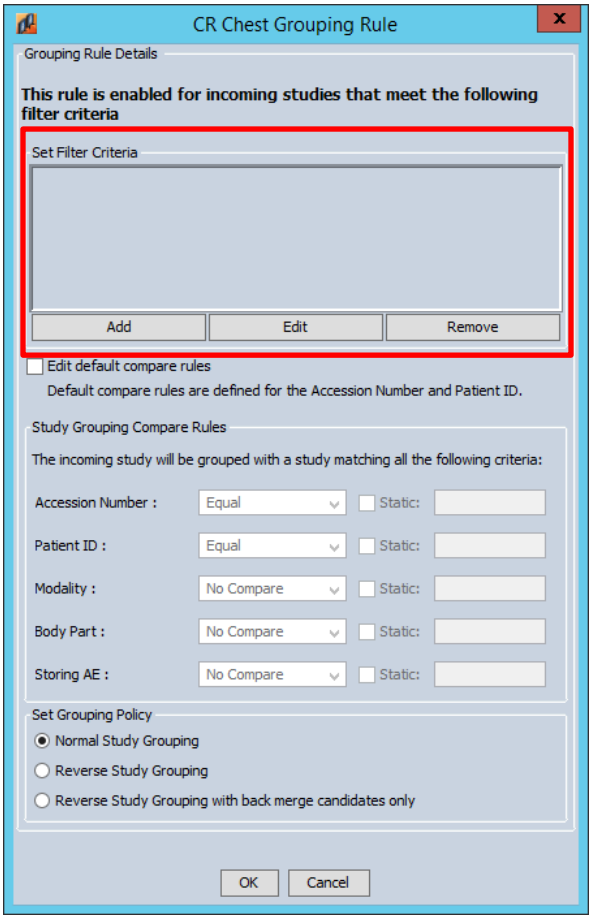


7. Select one of the following grouping policies:
   - **Normal study grouping** – If a match is found, the *existing* study determines the study instance ID.
   - **Reverse study grouping** – If a match is found, the *incoming* study determines the study instance ID. This is used, for example, if a report is created before the relevant images arrive from the modality.
   - **Reverse study grouping with back merge candidates only** – Searches for a match from studies that are marked explicitly as *back merge candidates.* If a match is found, the *incoming* study determines the study instance ID.

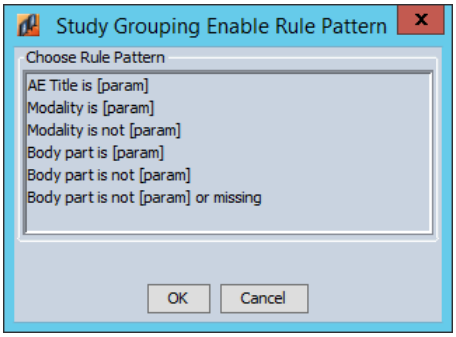
8. Click **OK** to return to the rule display area.
9. Repeat steps 2-8 to add additional rules that apply to all incoming studies.
10. Use the  and  buttons to change the order of the selected rules.
11. To define rules that apply to specific studies only, click **Add rule** in the lower section. The **Enter Rule Name** window appears.



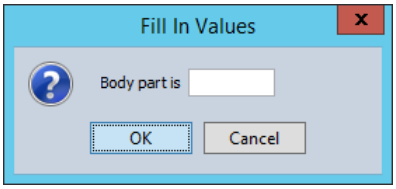
12. Type the rule name and click **OK**. The **Grouping Rule Details** window appears. It now includes the **Set Filter Criteria** section.



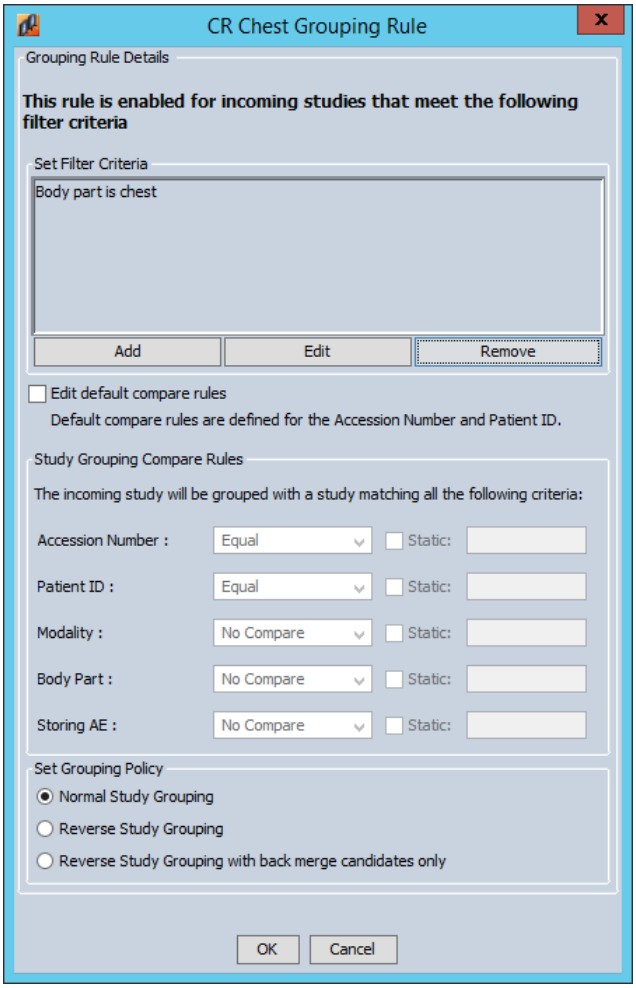
13. Click **Add**. The **Study Grouping Enable Rule Pattern** window appears.



14. Select the relevant rule pattern and click **OK**. The **Fill In Values** window appears.



15. Type the value and click **OK** to return to the **Grouping Rule Details** window.



16. Now you add the compare rules that are checked when the filter criteria are matched. See steps 2-8 for instructions on how to do this.
17. In the rule display area, use the  and  buttons to change the order of the selected rules.

    The study grouping mechanism runs the rules according to their priority, using the following logic:

    Run the first rule from the upper section (apply to all incoming studies).

    If a match is found, the matching studies are merged and the mechanism stops.

    If no match is found, continue to the remaining rules in the upper section until a match is found.

    If no match is found, continue to the rules in the lower section.

    Run the first rule from the lower section (apply to specific studies only), as follows:

    Run the filter rule on the incoming study.

    If filters match, run the relevant compare rule.

    If a match is found, the matching studies are merged and the mechanism stops.

    If no match is found, the mechanism stops.

    If no filter match is found, continue to the next rule in the lower section.

4.4.2.2 Editing a Study Grouping Rule

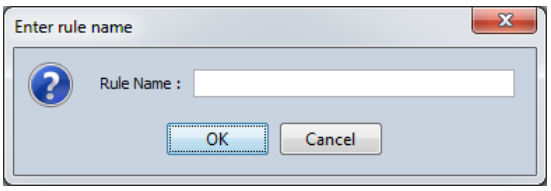
1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Study Grouping**.
2. In the rule display area in the right pane, select the rule and click **Edit**. The **Grouping Rule Details** window appears.
3. Edit the rule. See Section 4.4.2.1 Adding a Study Grouping Rule for details.

4.4.2.3 Removing a Study Grouping Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Study Grouping**.
2. In the rule display area in the right pane, select the rule and click **Remove**.
3. In the confirmation message that appears, click **Yes**.
4. The rule is removed from the rule display area.

4.4.2.4 Renaming a Study Grouping Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Study Grouping**.
2. In the rule display area in the right pane, select the rule and click **Rename**. The **Enter Rule Name** window appears.



3. Type the rule name and click **OK** to return to the rule display area.

4.4.3 Configuring Pre-Fetch Rules

You use pre-fetch rules to configure the study retrieval process so that specific studies can be retrieved in advance and be ready for the radiologist to read, at times when there is less demand on the server, or when a new study is stored.

The following types of pre-fetch rules can be configured:

- Study Arrives—The Workflow Manager receives images from an AE and queries the server for the patient's history.

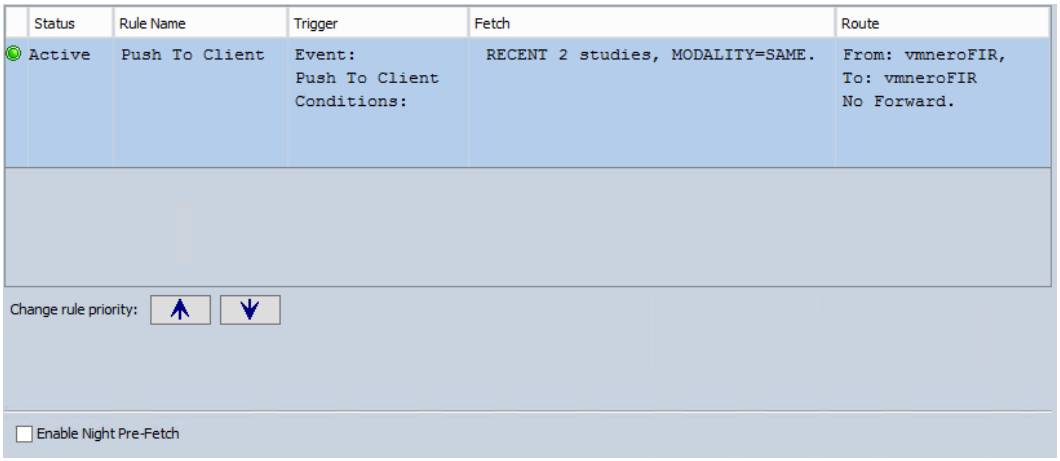
  This type of pre-fetch process is useful when there is no internal information system at the facility or in case of an emergency when there is no opportunity to retrieve the patient's history in advance.

- RIS Notification—IS Link informs the Workflow Manager when there is an order for a scan to be performed or when a patient is admitted to the facility.

  The details of the scan (for example, the body part to be scanned) are supplied to the Workflow Manager, if available. Based on this information, the appropriate studies are brought online before the new scan is performed.

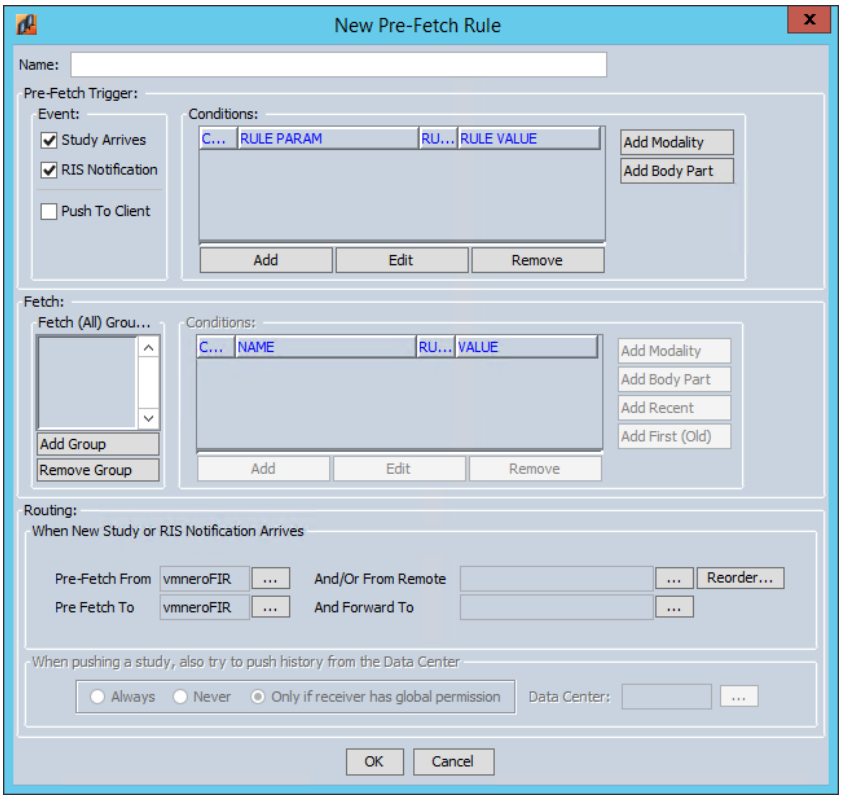
4.4.3.1 Adding a Pre-Fetch Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Pre-Fetch**. The rule display area appears in the right pane showing the out-of-the-box Push to Client rule. See Section 4.4.4 Configuring Push to Client Rules for more information.



2. From the System Configuration toolbar, click **Add**  or select **Add A Rule** from the right-click menu.

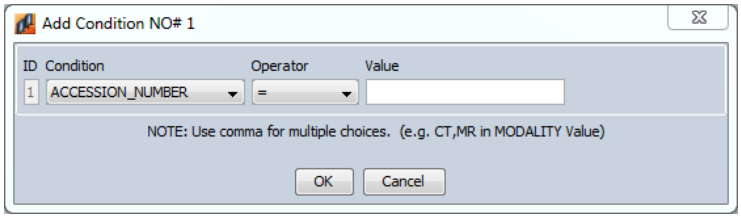
   The **New Pre-Fetch Rule** window appears.



3. In the **Name** box, type a name for the rule.
4. In the **Pre-Fetch Trigger** section, configure the events that trigger the pre-fetch:
   a. In the **Event** section, select from the following options:
      - **Study Arrives**—Pre-fetch is triggered when a study arrives at the Workflow Manager.
      - **RIS Notification**—Pre-fetch is triggered when there is an order for a scan to be performed or when a patient is admitted to the facility.

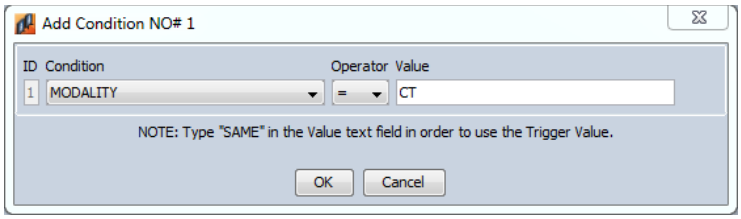
      Note: The **Push To Client** check box is used to define Push To Client rules. See Section 4.4.4 Configuring Push to Client Rules for more information.

   b. In the **Conditions** section, click **Add**, or use the predefined buttons, **Add Modality** or **Add Body Part**, and complete the relevant conditions for the rule.



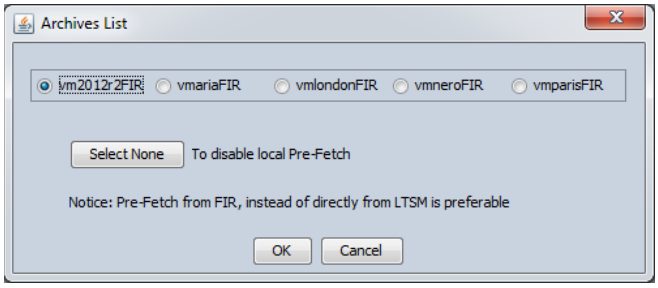
   c. Click **OK** to return to the **New Pre-Fetch Rule** window.
5. In the **Fetch** section, you configure groups of conditions that define which studies to retrieve from the backup device, as follows:
   a. Click **Add Group** and define the conditions for the Pre-Fetch function.

      For example, to transfer studies that relate to CT scans only, click **Add Modality**. In the **Add Condition** window, enter the value CT.

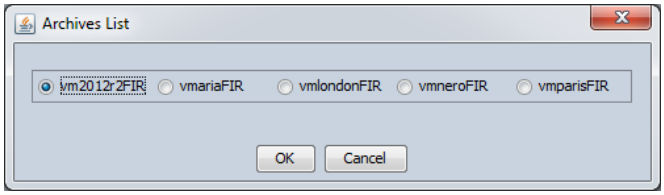


b. Configure additional conditions for the group, as required.

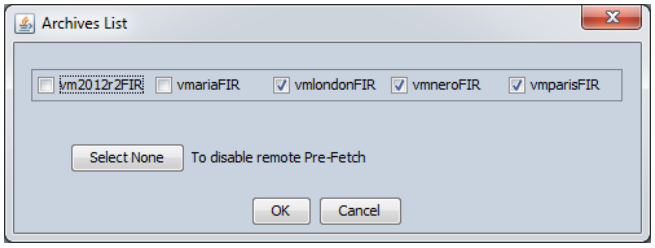
6. Repeat step 5 to configure additional groups, as required.
7. In the **Routing** section, you configure the pre-fetch archives used.
   In most cases, the main FIR is defined in both the **Pre-Fetch From** and **Pre-Fetch To** boxes.
   a. To configure a **local** pre-fetch archive:
      i. In the **Pre-Fetch From** box, click ….
      ii. In the **Archives List** window, select the archive from which to get the studies, or click **Select None** to disable the local pre-fetch mechanism.



      iii. Click **OK** to return to the **New Pre-Fetch Rule** window.
      iv. In the **Pre-Fetch To** box, click ….
      v. In the **Archives List** window, select the archive to which to forward the studies.



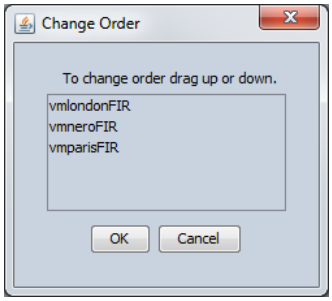
      vi. Click **OK** to return to the **New Pre-Fetch Rule** window.
   b. To configure a **remote** pre-fetch archive:
      i. In the **And/Or From Remote** box, click ….
      ii. In the **Archives List** window, select one or more archives from which to get the studies, or click **Select None** to disable the remote pre-fetch mechanism.



      iii. Click **OK** to return to the **New Pre-Fetch Rule** window.

iv. If you selected more than one archive, to change the order from which they are searched, click **Reorder**.

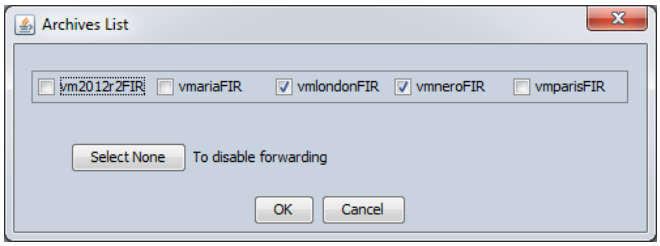
v. In the **Change Order** window, select one of the archives and drag it up or down, as required.



vi. Click **OK** to return to the **New Pre-Fetch Rule** window.

vii. In the **And Forward To** box, click ...

viii. In the **Archives List** window, select the archives to which to forward the studies or click **Select None** to disable the forwarding mechanism.



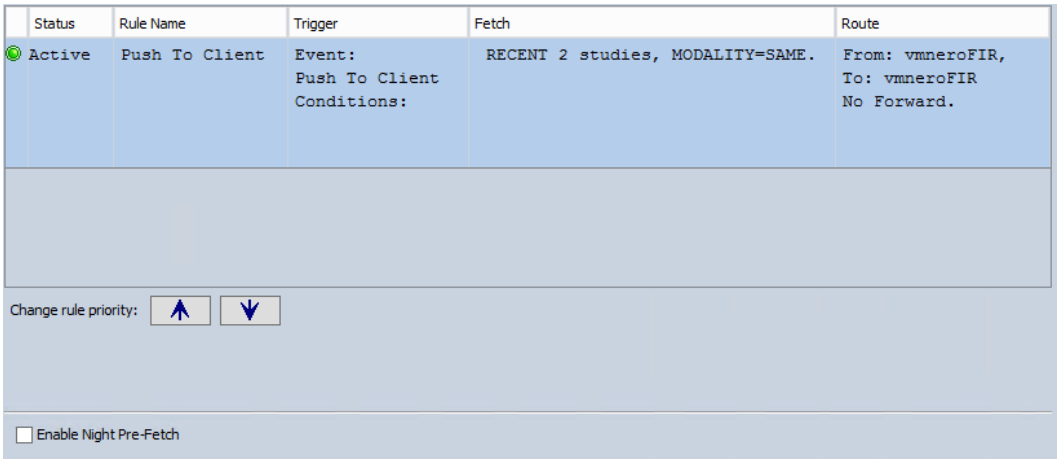
ix. Click **OK** to return to the **New Pre-Fetch Rule** window.

8. Click **OK** to return to the rule display area.
9. Repeat steps 2-7 to add additional pre-fetch rules.
10. Use the  and  buttons or the **Move Rule Up** and **Move Rule Down** from the right-click menu to change the order of the selected rules.
11. Click Save  .

4.4.3.2 Enabling Night Pre-Fetch

The Night Pre-Fetch process runs the night before the scheduled studies are due. You can enable this process, as follows:

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Pre-Fetch**. The rule display area appears in the right pane showing the out-of-the-box Push to Client rule.



2. Select the **Enable Night Pre-Fetch** check box.
3. Click **Save**  .

4.4.3.3 Activating and Deactivating Pre-Fetch Rules

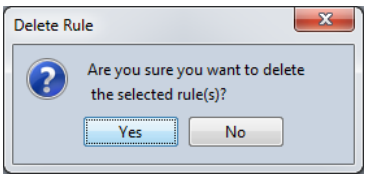
To activate or deactivate Pre-Fetch rules, select one or more rules and select **Activate Rule(s)** or **Deactivate Rule(s)** from the right-click menu.

4.4.3.4 Editing a Pre-Fetch Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Pre-Fetch**. The rule display area appears in the right pane.
2. Select the rule to edit and click **Edit**  or select **Edit Selected Rule** from the right-click menu.
3. In the **Update Pre-Fetch Rule** window, change the settings as required. See Section 4.4.3.1 Adding a Pre-Fetch Rule for more information.
4. Click **OK** to return to the rule display area.

4.4.3.5 Deleting a Pre-Fetch Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Pre-Fetch**. The rule display area appears in the right pane.
2. Select or more rules and click **Delete**  or select **Remove Rule(s)** from the right-click menu.
3. In the Delete Rule window, click **Yes** to confirm the deletion and return to the rule display area.



4.4.4 Configuring Push to Client Rules

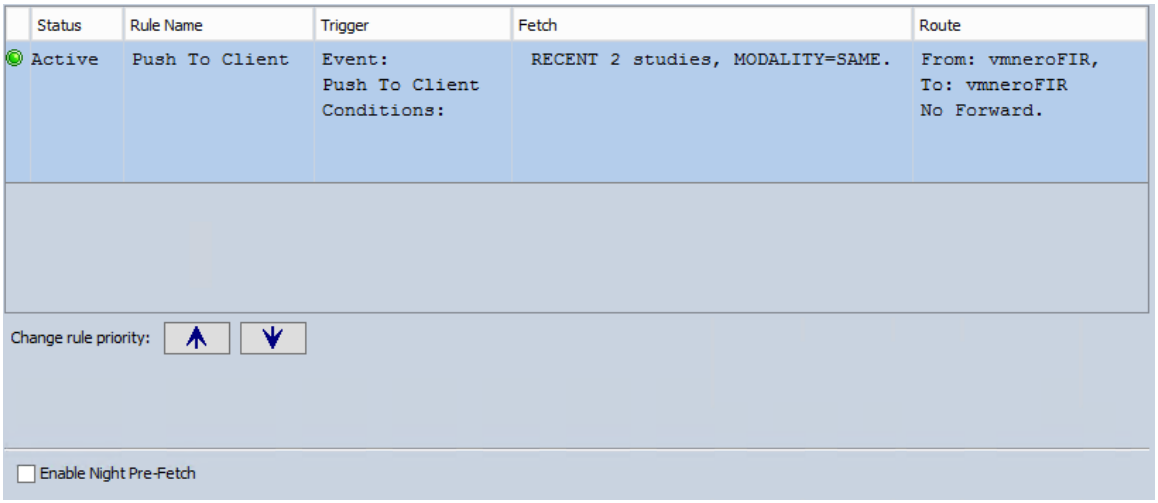
Radiologists can use the Push to Client function to transfer studies from the network to a local computer, such as a home PC, or to another physician. This is useful when the local computer is connected over a slow line and streaming cannot be used because images need to be loaded at a faster rate and without loss of quality.

When the radiologist transfers the studies, he or she can choose to transfer prior studies in addition to the current study.

You configure Push to Client rules to define which prior studies are transferred. You also need to define the user permissions to authorize which users can push studies. See Section 3.8.4.2 Workflow Permissions for more information.

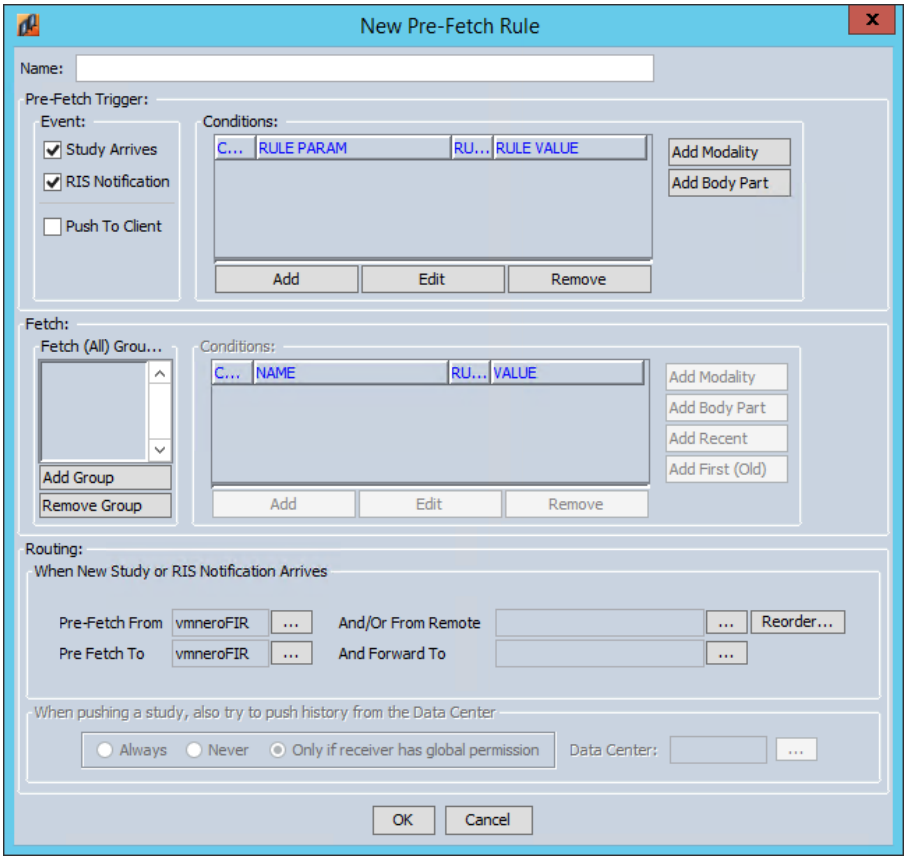
The out-of-the-box implementation already includes a Push to Client rule. You can modify this rule, or add additional rules, as follows:

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Pre-Fetch**. The rule display area appears in the right pane showing the out-of-the-box Push to Client rule.



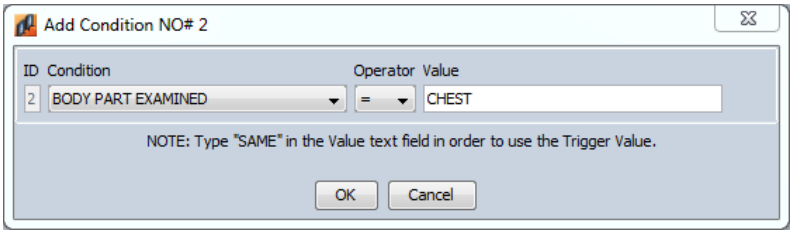
2. To add a new rule, from the System Configuration toolbar, click **Add**  .

   The **New Pre-Fetch Rule** window appears.



3. In the **Name** box, type a name for the rule.
4. In the **Pre-Fetch Trigger** section, clear the **Study Arrives** and **RIS Notification** check boxes and select the **Push To Client** check box.
5. In the **Fetch** section, click **Add Group** and define the conditions for the Push to Client function.

   For example, to transfer studies that relate to a specific body part, click **Add Body Part**. In the **Add Condition** window, enter a value for the body part and click **OK**.



   You can configure additional conditions for the group, as required.
6. Repeat step 5 to configure additional groups, as required.
7. In the **Routing** section, you configure whether users can push studies located on the data center or any other satellite connected to the grid. Select from the following options:
   - **Always—**The list of studies is a merged list based on the selected archive and the data center
   - **Never—**The list of studies is only based on the selected archive
   - **Only if receiver has global permission—**The list of studies is a merged list based on the selected archive and the data center, but only if the user has access permissions.

8. Click **OK** to return to the rule display area.
9. Repeat steps 2-8 to add additional Push to Client rules.
10. Use the  and  buttons to change the order of the selected rules.
11. Click Save  .

Note: In addition to the Push to Client rules, you can also define parameters for the local computer in the Central Configuration. For example, you can define the maximum size of the repository and the number of days to keep pushed studies. For more information on these parameters, contact Customer Service.

4.4.5 Configuring Icons Settings

You configure the *image* icon creation strategy in the **Workflow Manager Configuration > Icons Settings** screen. It is recommended to leave the default values as is, or consult with Carestream Professional Services personnel before making changes.

Note: Series icons are created automatically, and the configuration is not done in this screen.

4.4.6 Configuring Compression Settings

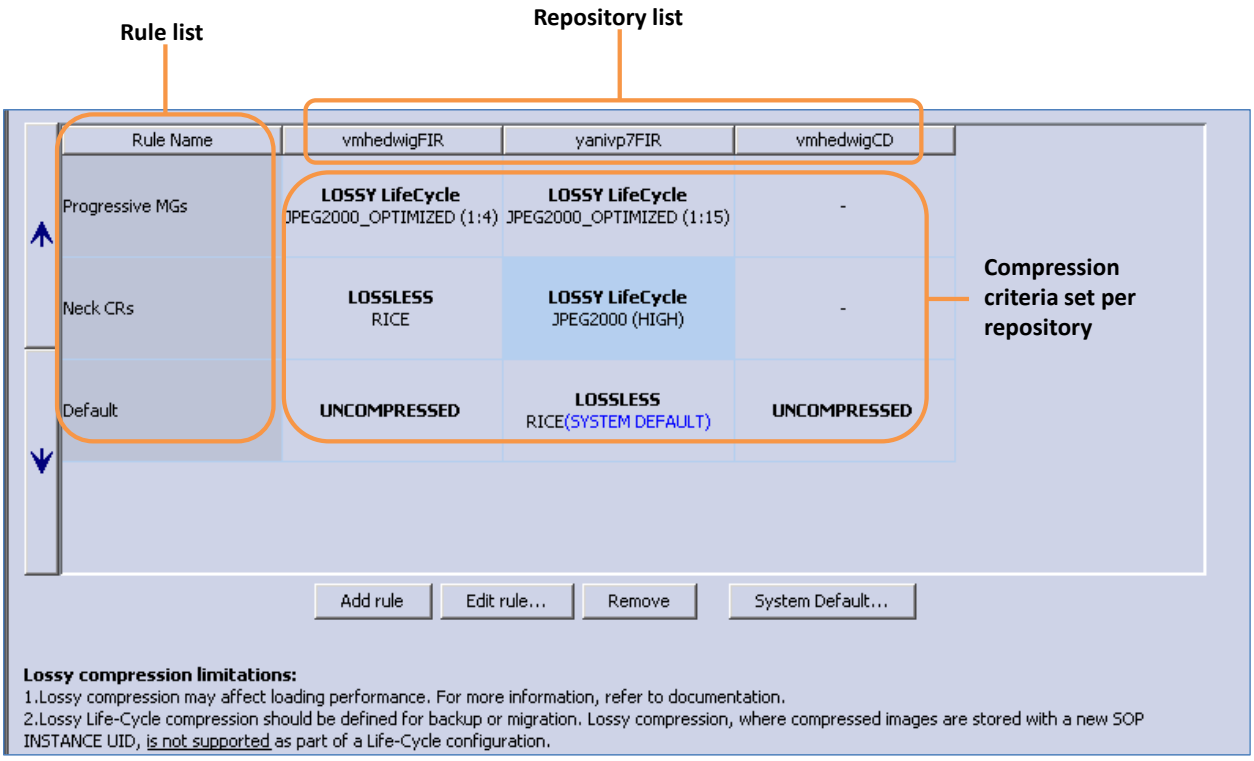
Modalities are generating more and more images of increasing resolution, contributing to the large volume of digital data that requires storage. Reducing the file size means that more images can be stored in a given amount of memory space, and images can be transferred and downloaded more quickly.

Compression can be used to reduce image file sizes using the following compression techniques:

- Lossless—all image information originally in the file remains after the file is uncompressed. Lossless compression reduces file sizes by a factor of 2 or 3.
- Lossy—reduces the file size by permanently removing certain information. You can decide how much loss to introduce and make a trade-off between file size and image quality. When the file is uncompressed, only part of the original image remains, however, this is often not noticeable. Lossy compression often reduces file sizes by a factor of 10 or more.

See Section 4.4.6.5 Compression Methods for more information on the compression methods available.

You use the System Configuration tool to configure compression rules that determine which images are compressed and the compression method. The compression rules are displayed in a table, as shown in the following figure.



Each row in the table represents a compression rule, containing one or more compression criteria. The rules are run in order until a match is found. If no match is found, then the default compression is used.

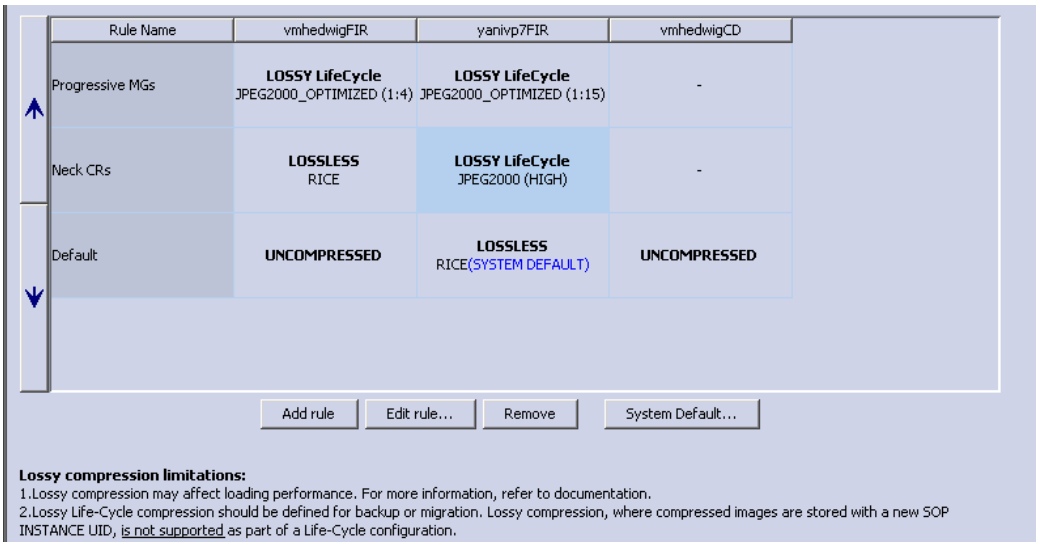
Each column in the table represents a repository. The main storage repository appears first, followed by additional repositories.

When you configure compression rules, the information is reflected in the Central Configuration in the following location:

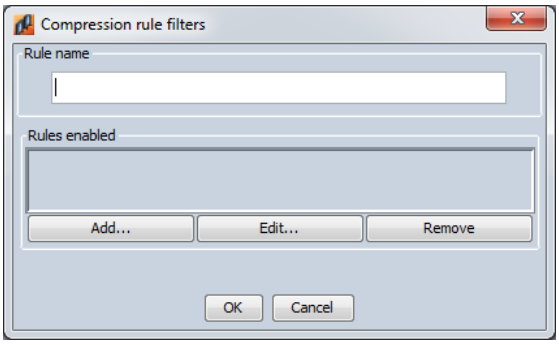
```
imaginet\system\applications\medistore\fir\compression
```

4.4.6.1 Adding a Compression Rule

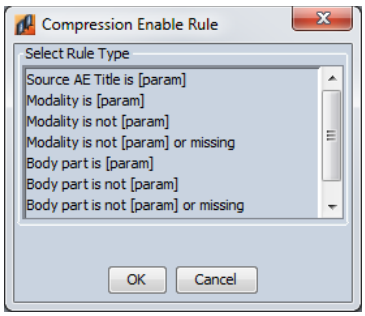
1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Compression Settings**. The rule display area appears in the right pane.



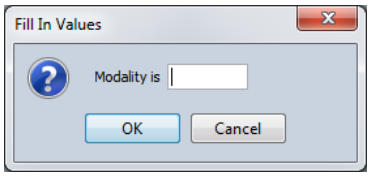
2. From the System Configuration toolbar, click **Add**  or click the **Add rule** button. The **Compression rule filters** window appears.



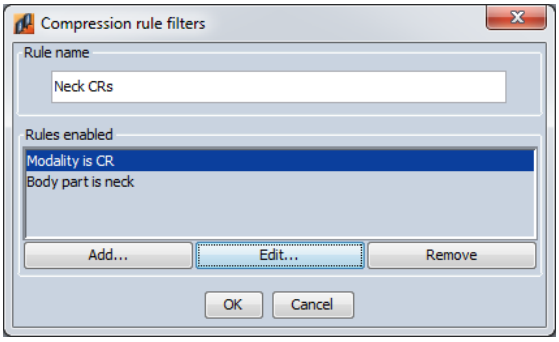
3. In the **Rule name** box, type a name for the rule.
4. In the **Rules enabled** section, you configure which images are compressed:
   a. Click **Add**.
   b. In the **Compression Enable Rule** window, select the rule type and click **OK**.



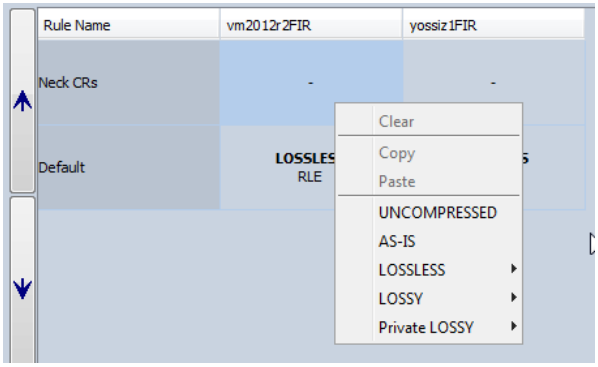
   c. In the **Fill In Values** window, type the value that matches the rule type and click **OK** to return to the **Compression rule filters** window.



In the following example, a rule is defined for selecting CR images of the neck.



5. Click **OK**. The new rule appears in a new row in the rule display area.
6. In the first cell of the new row, right-click and select the compression method for the new rule for the first repository:



See Section 4.4.6.5 Compression Methods for an explanation of the possible options.

Note: You can copy and paste cells in the table.

7. Repeat step 6 for each of the repositories.
8. Repeat steps 2-7 to add additional compression rules.
9. Use the  and  buttons to change the order of the selected rules.
10. Click **Save**  .

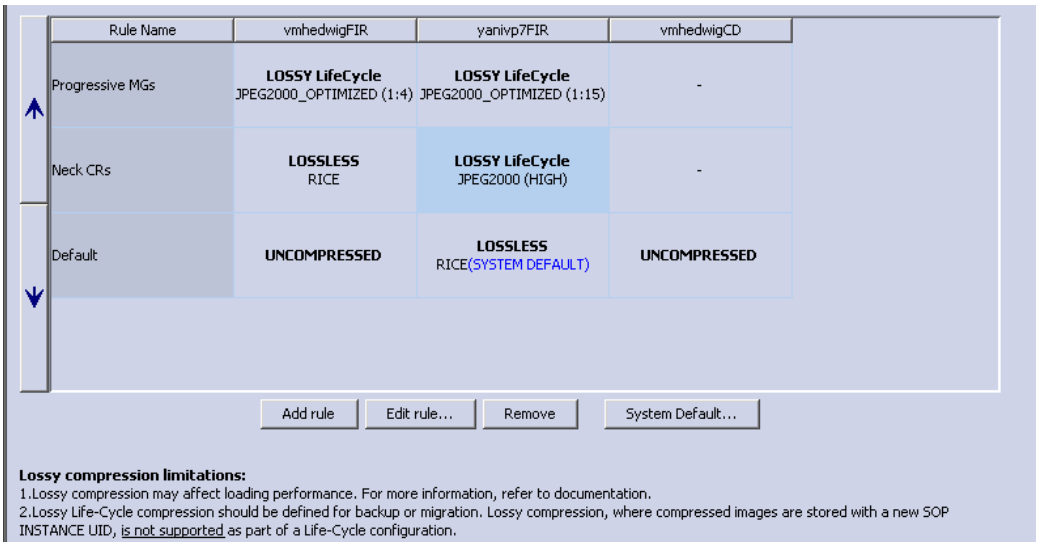
4.4.6.2 Working with Default Compression Rules

When a new repository is installed, a default compression rule is automatically added (usually lossless RICE compression) and appears in the last row of the table. When the rules are run, if no match is found, the default compression method is used.

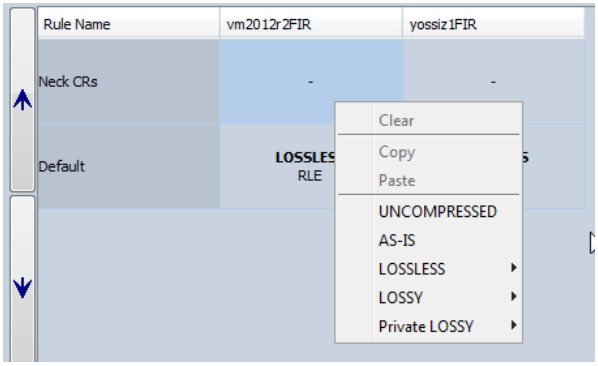
You can remove the compression method in the default rule. To do this, right-click the cell and select **Clear**. In this case, when the rules are run, if no match is found, the **system** default compression method is used.

4.4.6.3 Editing a Compression Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Compression Settings**. The rule display area appears in the right pane.



2. Select the rule to edit and, from the System Configuration toolbar, click **Edit**  or click the **Edit rule** button.
3. In the **Compression rule filters** window, change the rule parameters as required.
4. Click **OK**.
5. To change the compression method, right-click the cell and select the required compression method.



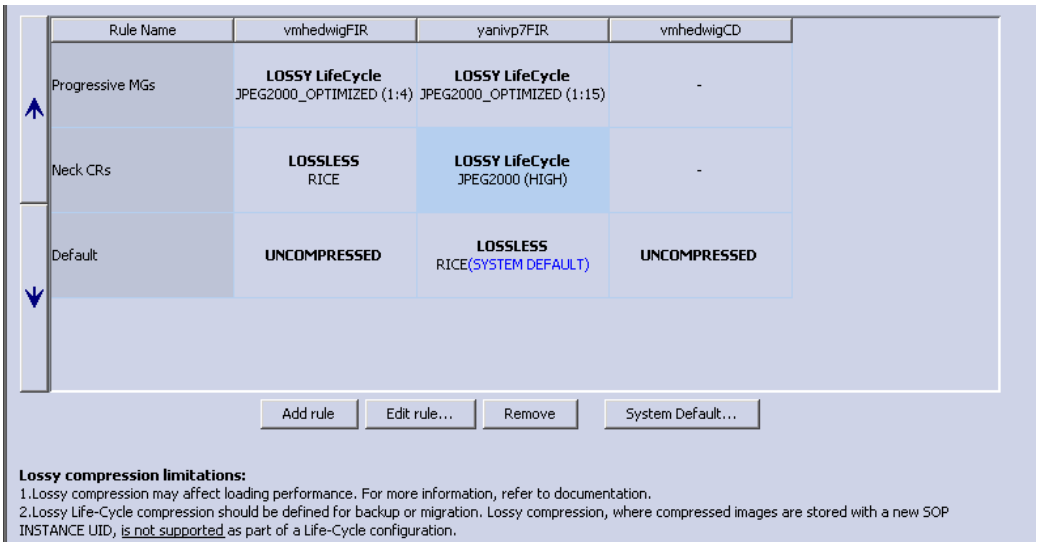
See Section 4.4.6.5 Compression Methods for an explanation of the possible options.

Note: You can copy and paste cells in the table.

6. Click **Save**  .

4.4.6.4 Deleting a Compression Rule

1. In the left pane of the System Configuration tool, navigate to **Workflow Manager Configuration > Compression Settings**. The rule display area appears in the right pane.



2. Select the rule and, from the System Configuration toolbar, click **Delete**  or click the **Delete** button.

   The rule is removed from the rule display area.

3. Click **Save**  .

4.4.6.5 Compression Methods

The following table lists the compression methods that that can be used to compress image files.

Compression Method	Description
Uncompressed	Image files are not compressed.
As-Is	Image files are left as-is.
Lossless	Image files are compressed without reducing image quality. When a file is uncompressed, all the original information is restored. The following types of lossless compression are available: • RICE • RLE • JPEG • JPEG 2000 • JPEG 2000 Optimized

Compression Method	Description
Lossy	Image files are compressed and some information is lost. When a file is uncompressed, only part of the original image remains, however, this is often not noticeable. The following types of lossy compression are available: • JPEG • JPEG 2000 • JPEG 2000 Optimized For JPEG and JPEG 2000, you can decide on the degree of compression: high, medium, default, or low. When the value is high, the file is more compressed. When the value is low, the file is less compressed. For JPEG 2000 Optimized, you select the compression ratio. Lossy compressed images are stored with a new SOP instance UID and comply with the DICOM standard.
Private Lossy	Private lossy compression is used when a storage life cycle is defined. For example, when images are initially stored using lossless optimized compression. After 3 years, images are migrated to another repository and are compressed using lossy compression. After 4 more years, images are compressed further, migrated to another repository, and deleted from the previous repository. Lossy compressed images are stored with the same SOP instance UID. For more information on using this compression method, contact Customer Service.

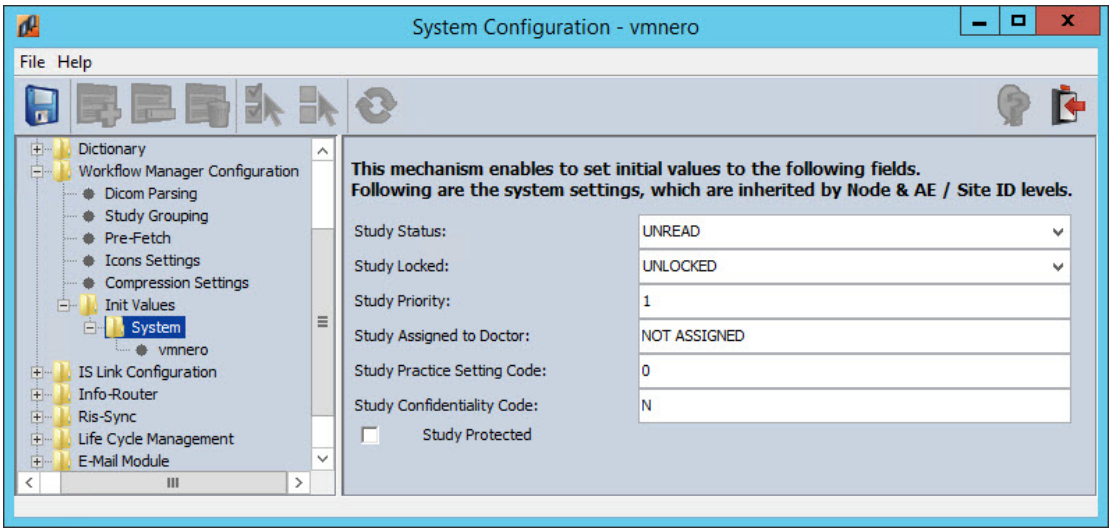
4.4.7 Configuring Initial Values

You can set initial values for incoming studies that do not already have values assigned. The values can be assigned at the system, node, site, or AE levels. For example, you can set the initial study status for all incoming studies to be UNREAD, or you can assign all incoming studies for a specific site to a particular doctor.

System-level values are automatically inherited by the levels below, unless they are modified at any of the node, site, or AE levels.

4.4.7.1 Configuring Initial Values at the System Level

1. In the left pane of the System Configuration tool, go to **Workflow Manager Configuration > Init Values > System**.



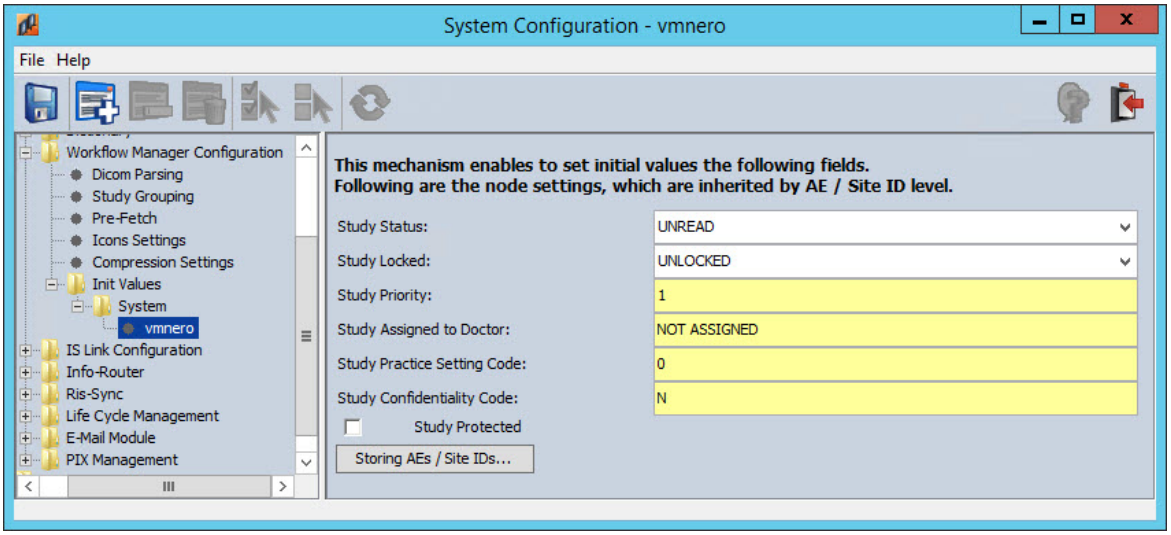
2. In the right pane, complete the following fields, as appropriate:
    - Study Status—The status assigned to incoming studies
    - Study Locked—Indicates whether the incoming study is locked or unlocked.
    - Study Priority—The priority of the study. The highest priority is 1.
    - Study Assigned to Doctor—Indicates whether the study is assigned to a particular doctor.
    - Study Practice Setting Code—The department code used in vendor-neutral archiving scenarios. Possible values are:
        - 0—Radiology
        - 100—Cardiology
        - 200—Endoscopy
        - 300—Gastroenterology
        - 400—Dermatology
        - 500—Opthalmology
        - 600—Pathology

- Study Confidentiality Code—The data sensitivity, which is used when applying access control rules. Possible values are:
  - N—Normal
  - R—Restricted
  - V—Very Restricted
- Study Protected—Indicates whether the study is protected from auto-deletion.

3. When you have finished configuring the initial values, save your changes and restart the affected services.

4.4.7.2 Configuring Initial Values at the Node, Site and AE Levels

1. In the left pane of the System Configuration tool, go to **Workflow Manager Configuration > Init Values > System** and select the relevant node. In this example, **vmnero** is selected.

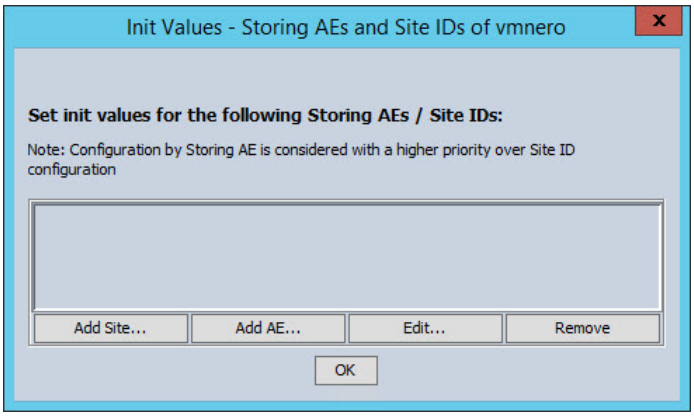


2. In the right pane, complete the appropriate fields, as described in Section 4.4.7.1 Configuring Initial Values at the System Level.

NOTE: The color of the fields changes according to their status, as follows:

- Yellow indicates that the setting is inherited from the system-level settings.
- White indicates that the value has been modified and is defined at the node level.

3. To configure initial values at the site and AE levels, click the **Storing AEs / Site IDs** button.
4. In the **Init Values** window, click the **Add Site** or **Add AE** button, as appropriate.



5. In the window that opens, enter the site ID or AE title and click **OK**.
6. In the left pane, select the site or AE that you just added.
7. In the right pane, complete the appropriate fields, as described in Section 4.4.7.1 Configuring Initial Values at the System Level.

   NOTE: The color of the fields changes according to their status, as follows:

   - Yellow indicates that the setting is inherited from the node-level settings.
   - White indicates that the value has been modified and is defined at the site or AE level.
8. When you have finished configuring the initial values, save your changes and restart the affected services.

4.5 Configuring IS Link

IS Link is a configurable HL7 interface engine that provides seamless integration between CARESTREAM Vue PACS and hospital information systems (HIS), radiology information systems (RIS), and other healthcare information systems. Specifically, IS Link provides CARESTREAM Vue PACS with patient demographic, visit, and order information, and enables the retrieval of clinical reports.

IS Link includes the following main processes:

- **Listener**—Receives HL7 messages from RIS/HIS and stores them in a message queue ready for the Converter process.
- **Converter**—Fetches HL7 messages from the message queue, processes the messages, and then uploads the relevant information to the IS Link database.

IS Link supports the following HL7 messages:

- ADT—Admission, discharge, transfer messages
- ORM O01—General order message
- ORU R01—Observational results

For more information on the HL7 communication protocol, see *CARESTREAM Vue PACS HL7 Interface Specifications*.

You can use the System Configuration tool to configure the following IS Link features:

- Listener process
- Converter process
- Database
- Reports and orders

- Report parser
- Queues and notifications

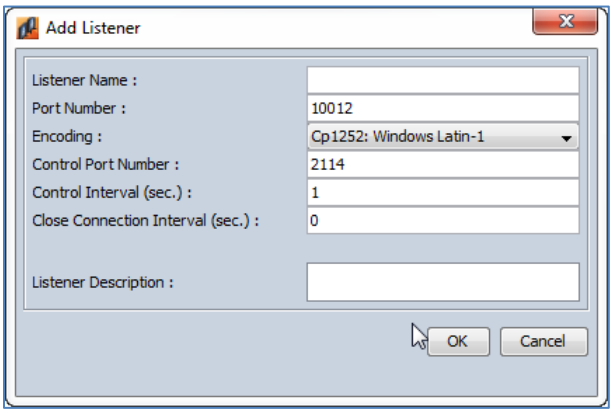
4.5.1 Configuring the Listener Process

The Listener process receives HL7 messages from RIS or HIS and places them in a message queue in the IS Link database.

You use the System Configuration tool to add listener processes and configure parameters, such as the port for TCP/IP connections from clients.

4.5.1.1 Adding a Listener Process

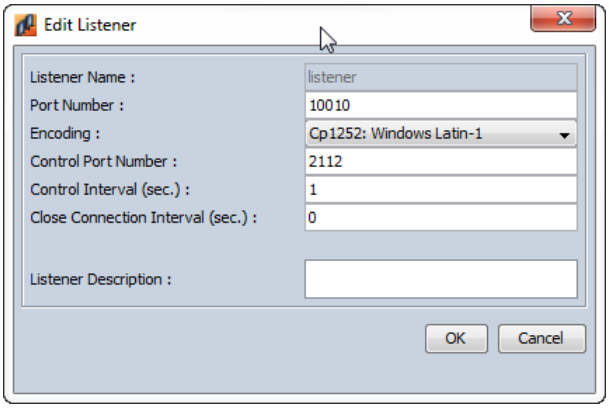
1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Listeners**.
2. From the System Configuration toolbar, click **Add**  or select **Add** from the right-click menu. The **Add Listener** window appears.



3. Configure the listener properties, as follows:
   - **Listener Name**—The name of the listener process.
   - **Port Number**—The port used by the listener process for TCP/IP connections.
   - **Encoding**—The character encoding used.
   - **Control Port Number**—The control port, which is used to check if the listener process is up. The default is 2114.
   - **Control Interval (sec)**—The frequency for checking whether the control port is in use, in seconds.
   - **Close Connection Interval (sec)**—The period of time after which the non-active connection is closed.
   - **Listener Description**—A description of the listener process.
4. Click **OK**. The listener appears in the right pane.
5. Click **Save**  , then restart the affected services.

4.5.1.2 Editing Listener Configuration Parameters

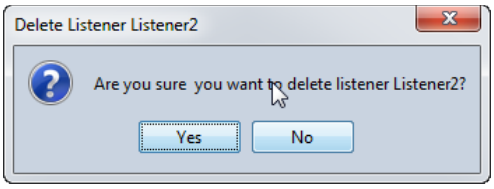
1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Listeners**.
2. In the right pane, select the listener process to edit from the **Listeners** drop-down list.
3. From the System Configuration toolbar, click **Edit**  or select **Edit** from the right-click menu. The **Edit Listener** window appears.



4. Edit the listener parameters as required. See Section 4.5.1.1 Adding a Listener Process for details.
5. Click **OK**.
6. Click **Save**  , then restart the affected services.

4.5.1.3 Deleting a Listener Process

1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Listeners**.
2. In the right pane, select the listener process to delete from the **Listeners** drop-down list.
3. From the System Configuration toolbar, click **Delete**  or select **Delete** from the right-click menu.
4. In the **Delete Listener** window, click **Yes** to confirm the deletion and return to the display area.



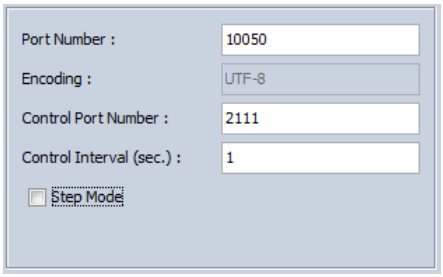
5. Click **Save**  , then restart the affected services.

4.5.2 Configuring the Converter Process

The Converter process fetches HL7 messages from the message queue, separates each message into segments, and then parses them to the relevant IS Link database tables. When message processing is complete, the Converter sends event notifications to the relevant enabled notification queues.

You use the System Configuration tool to configure the converter process, as follows:

1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Converter**. The configuration area appears in the right pane.



2. In the right pane, configure the converter properties, as follows:
   - **Port Number**—The port used by the converter process for TCP/IP connections.
   - **Encoding**—The character encoding used.
   - **Control Port Number**—The control port, which is used to check if the converter process is up. The default is 2111.
   - **Control Interval (sec)**— The period of time after which the non-active connection is closed.

   Do not select the step mode check box, as it is not in use.

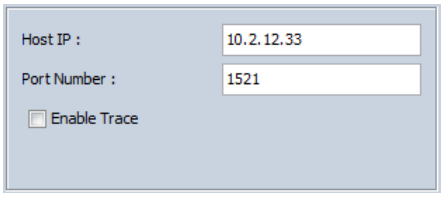
3. Click **Save**  , then restart the affected services.

4.5.3 Configuring the IS Link Database

IS Link receives and translates HL7 data from RIS or HIS and uploads the translated data in the IS Link database.

You use the System Configuration tool to configure the IS Link database, as follows:

1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Database**. The configuration area appears in the right pane.



2. In the right pane, configure the converter properties, as follows:
   - **Host IP**—The host IP of the IS Link database.
   - **Port Number**—The port number. The default is 1521.

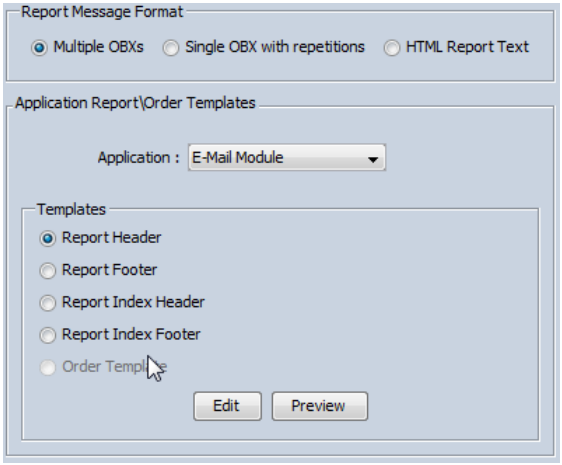
3. Click **Save**  , then restart the affected services.

4.5.4 Editing Report and Order Templates

IS Link enables the end user, such as a radiologist, to view clinical reports using the CARESTREAM PACS Client. The report information is stored in the IS Link database and can be retrieved as required.

You use the System Configuration tool to edit the report and order templates, as follows:

1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Reports & Orders**. The display area appears in the right pane.



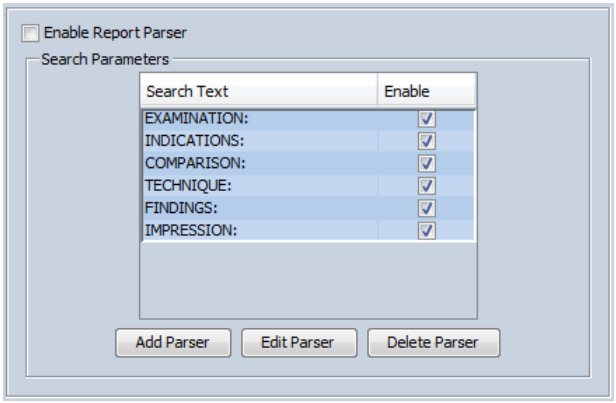
2. In the Report Message Format section, select from the following options:
   - Multiple OBXs
   - Single OBX with repetitions
   - HTML Report Text
3. In the **Application Report/Order Templates** section, select the application used to view the report from the drop-down list.
4. In the **Templates** section, select the report template to edit. The options available depend on the application selected in step 3.
5. Click **Edit**. The **Edit Record** window appears in which you can change the format of the selected template.
6. When you have finished making your changes, click **OK** to return to the display area.
7. Click **Save**  , then restart the affected services.

Note: You can use the **Preview** option to preview the templates after making your changes.

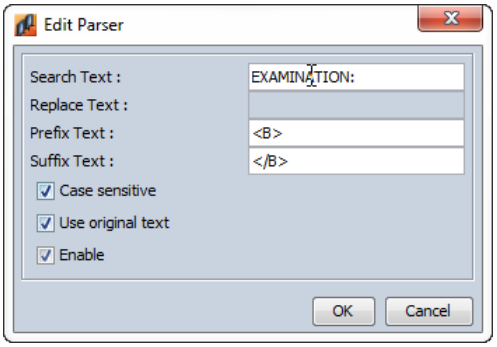
4.5.5 Enabling Report Parsing

You use the System Configuration tool to enable report parsing and to define report parsing parameters.

1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Report Parser**. The display area appears in the right pane.



2. To enable report parsing, select the **Enable Report Parser** check box.
3. In the **Search Parameters** section, select or deselect the **Enable** check box for each parsing element.
4. To edit the parsing parameters for a specific parsing element, select the parsing element from the **Search Text** list and click **Edit Parser**. The **Edit Parser** window appears.

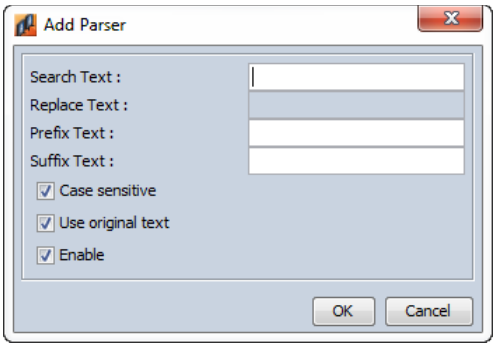


5. Configure the parsing parameters, as required, and click **OK** to return to the display area.
6. Click **Save**  , then restart the affected services.

4.5.5.1 Adding a Parsing Element

You use the System Configuration tool to add new parsing elements, which can be used to modify text fragments in reports.

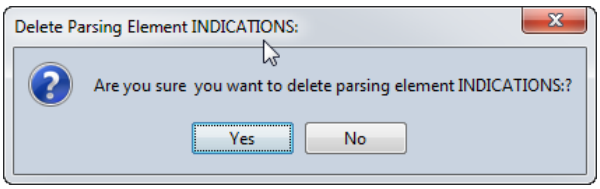
1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Report Parser**. The display area appears in the right pane.
2. In the **Search Parameters** section, click **Add Parser**. The **Add Parser** window appears.



3. In the **Add Parser** window, configure the parsing element properties, as follows:
   - **Search Text**—The text that you want to modify.
   - **Replace Text**—The replacement text. This option is only available if the **Use original text** check box is not selected.
   - **Prefix Text**— The text to insert before the text fragment. For example, to bold a text fragment, use the tag as a prefix.
   - **Suffix Text**— The text to insert after the text fragment. For example, if you used the tag as a prefix, enter tag as a suffix.
   - **Case sensitive**—Indicates whether the parser is case-sensitive.
   - **Use original text**—Indicates whether to use leave the original text as is. If no, use the **Replace Text** box to define the replacement text.
   - **Enable**—Indicates whether the parsing element is enabled.
4. Click **OK** to return to the display area.
5. Click **Save**  , then restart the affected services.

4.5.5.2 Deleting a Parsing Element

1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Report Parser**. The display area appears in the right pane.
2. From the **Search Text** list, select the parsing element to delete and click **Delete Parser**.
3. In the **Delete Parsing Element** window, click **Yes** to confirm the deletion and return to the display area.



4. Click **Save**  , then restart the affected services.

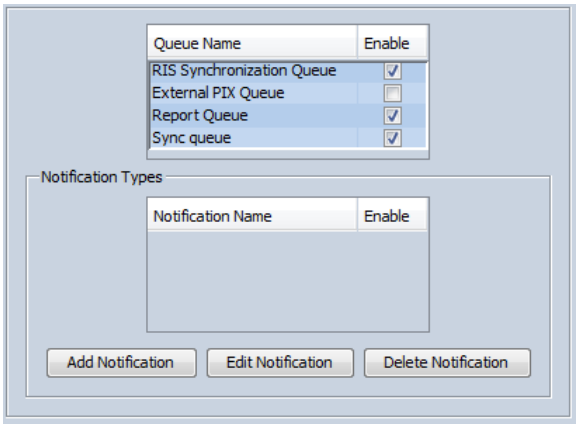
4.5.6 Configuring Queues and Notifications

When message processing is complete, the converter sends the event notifications to the relevant notification queues.

You use the System Configuration tool to configure the notifications and enable the relevant queues.

4.5.6.1 Adding a Notification

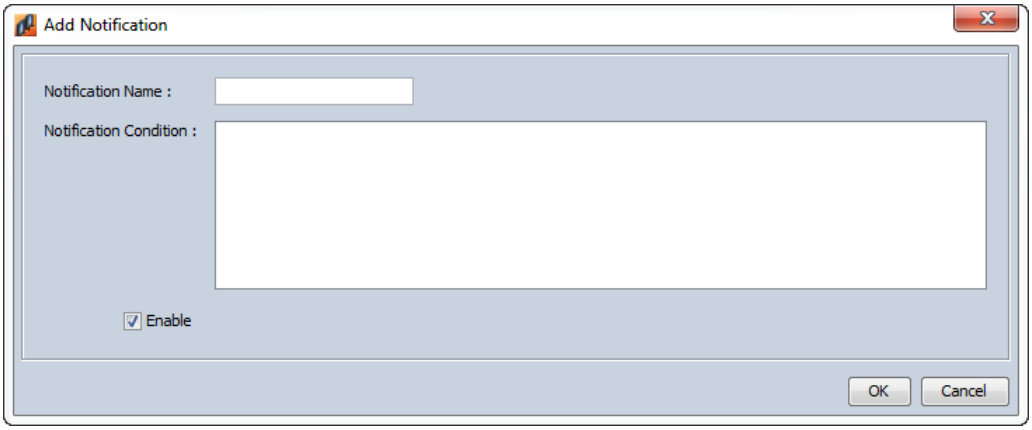
1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Queues & Notifications**. The configuration area appears in the right pane.



2. Select a queue from the **Queue Name** list.

   The list of notifications appears under the Notification Name list. The check box indicates whether the notification is enabled.

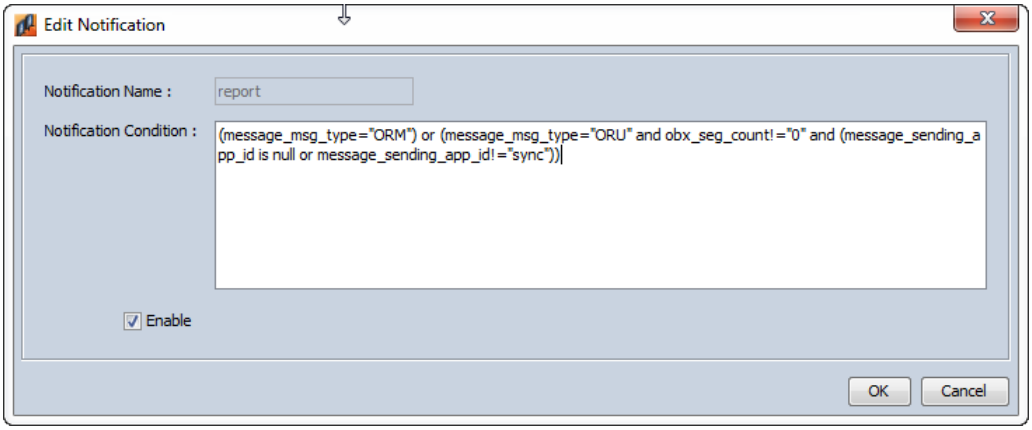
3. Click **Add Notification**. The **Add Notification** window appears.



4. In the **Notification Name** box, type the name of the notification.
5. In the **Notification Condition** box, type the condition for the notification.
6. Select the **Enable** check box and click **OK** to return to the display area.
7. Click **Save**  , then restart the affected services.

4.5.6.2 Editing a Notification

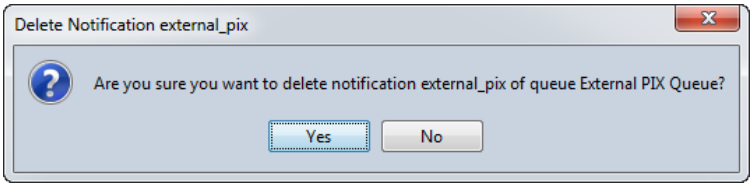
1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Queues & Notifications**.
2. In the right pane, select the notification to edit in the Notification Types section and click **Edit Notification**.
3. The **Edit Notification** window appears.



4. In the **Notification Condition** box, edit the condition for the notification, as required.
5. Click **OK**.
6. Click **Save**  , then restart the affected services.

4.5.6.3 Deleting a Notification

1. In the left pane of the System Configuration tool, navigate to **IS Link Configuration > Queues & Notifications**.
2. In the right pane, select the notification to delete in the Notification Types section and click **Delete Notification**.
3. In the **Delete Notification** window, click **Yes** to confirm the deletion and return to the display area.



4. Click **Save**  , then restart the affected services.

4.6 Configuring HL7-PACS Field Mapping

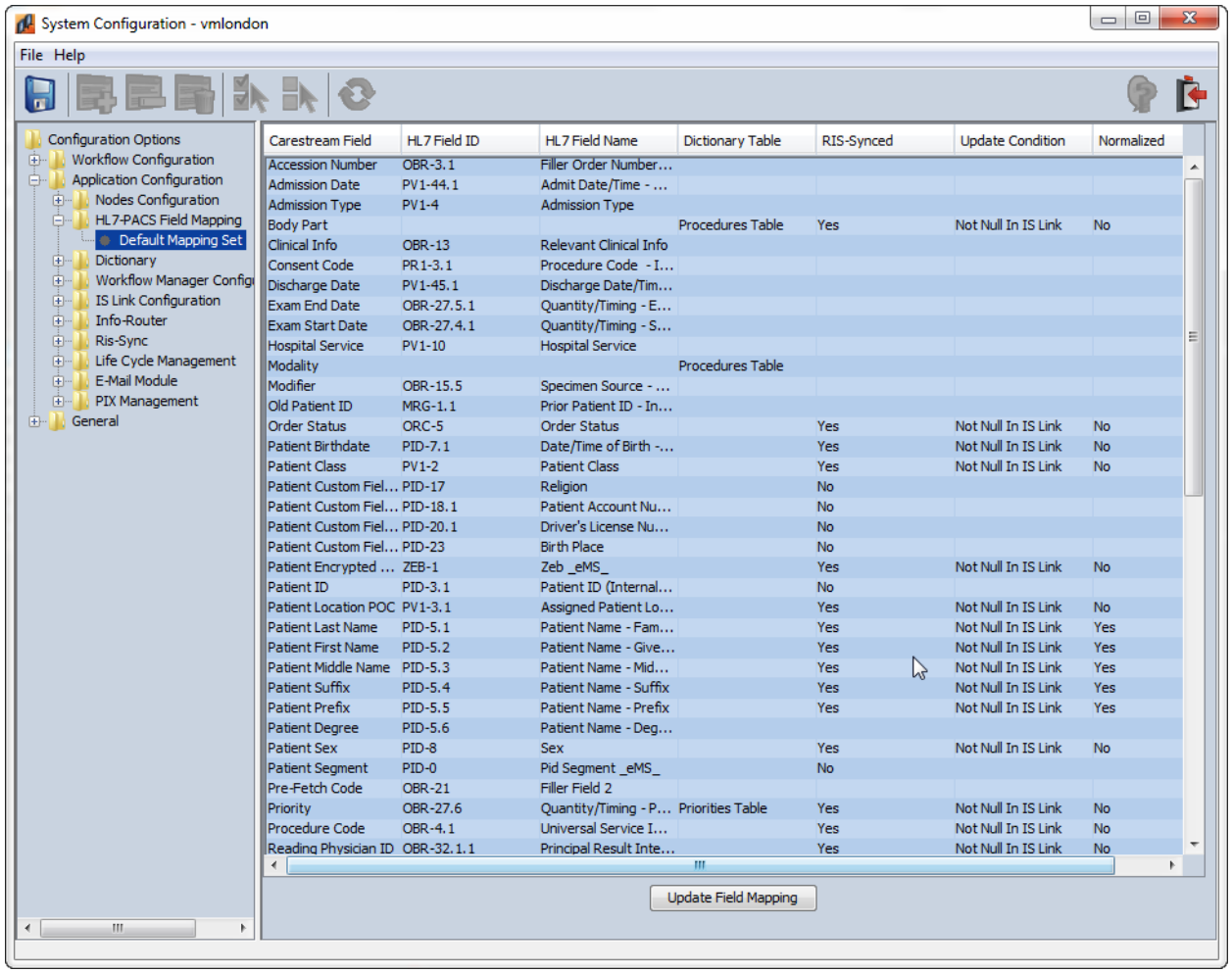
IS Link processes HL7 messages from RIS and HIS and uploads the relevant information to the IS Link database. This information can then be used by the RIS Synchronization process to update the Workflow Manager.

In the out-of-the-box implementation, a default mapping set defines which HL7 fields are mapped to which DICOM fields.

You can use the System Configuration tool to view the default mapping set and modify the field mappings, if required. You can also define whether the HL7 field is modified using a dictionary table and whether the Workflow Manager should be notified of changes to the HL7 field using the RIS Synchronization process.

For example, for the Exam Start Date field, RIS sends OBR-36 instead of the expected OBR-27.4.1. You can change the default field mapping of the Exam Start Date field from OBR-27.4.1 to OBR-36.

The HL7-PACS field mapping set is shown below.



Each row in the table displays the mapping of an HL7 field to a field in the IS Link database. It includes the following information:

- Carestream Field—The destination field in the IS Link database. This is the DICOM tag.
- HL7 Field ID—The unique ID of the source HL7 field.
- HL7 Field Name—The name of the source HL7 field.

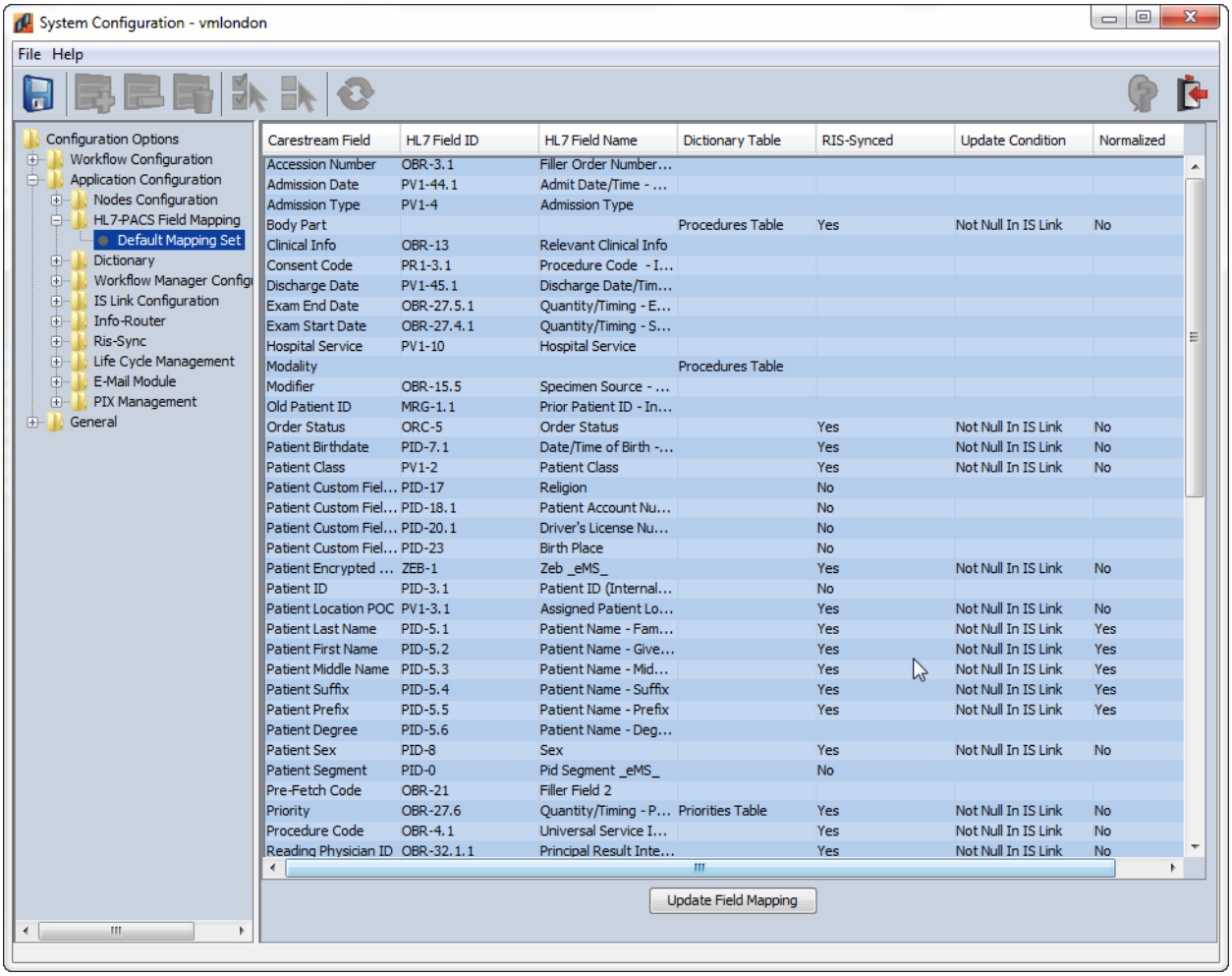
- Dictionary Table—Indicates whether the HL7 field is converted through a dictionary table. Possible options are:
    - Simple mapping table, which converts one value into another. For example the Priorities table.
    - Complex mapping table, in which you define a number of columns. The out-of-the-box implementation includes the Procedures and Study Status Translations tables.

  For more information on using dictionary tables, see Section 4.6.2 Using Dictionary Tables.
- RIS-Synced—Indicates whether to notify the Workflow Manager of updates to this field using the RIS Synchronization process, for example, when the patient details are updated.
- Update Condition—The condition that defines when RIS synchronization takes place.
- Normalized—Indicates whether the RIS value is dicomized during RIS synchronization.

For more information on the HL7 fields and the communication protocol, see *CARESTREAM Vue PACS HL7 Interface Specifications*.

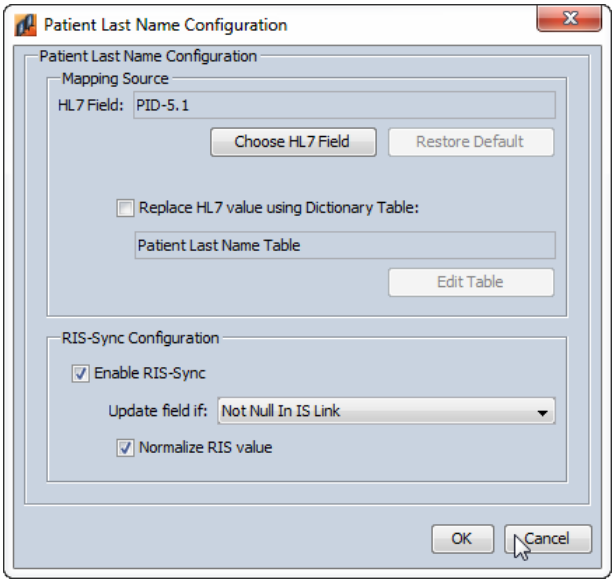
4.6.1 Modifying the HL7-PACS Field Mappings

1. In the left pane of the System Configuration tool, navigate to **HL7-PACS Field Mapping > Default Mapping Set**. The display area appears in the right pane.



Carestream Field	HL7 Field ID	HL7 Field Name	Dictionary Table	RIS-Synced	Update Condition	Normalized
Accession Number	OBR-3.1	Filler Order Number...				
Admission Date	PV1-44.1	Admit Date/Time - ...				
Admission Type	PV1-4	Admission Type				
Body Part			Procedures Table	Yes	Not Null In IS Link	No
Clinical Info	OBR-13	Relevant Clinical Info				
Consent Code	PR1-3.1	Procedure Code - I...				
Discharge Date	PV1-45.1	Discharge Date/Tim...				
Exam End Date	OBR-27.5.1	Quantity/Timing - E...				
Exam Start Date	OBR-27.4.1	Quantity/Timing - S...				
Hospital Service	PV1-10	Hospital Service				
Modality			Procedures Table			
Modifier	OBR-15.5	Specimen Source - ...				
Old Patient ID	MRG-1.1	Prior Patient ID - In...				
Order Status	ORC-5	Order Status		Yes	Not Null In IS Link	No
Patient Birthdate	PID-7.1	Date/Time of Birth -...		Yes	Not Null In IS Link	No
Patient Class	PV1-2	Patient Class		Yes	Not Null In IS Link	No
Patient Custom Fiel...	PID-17	Religion		No		
Patient Custom Fiel...	PID-18.1	Patient Account Nu...		No		
Patient Custom Fiel...	PID-20.1	Driver's License Nu...		No		
Patient Custom Fiel...	PID-23	Birth Place		No		
Patient Encrypted ...	ZEB-1	Zeb _eMS_		Yes	Not Null In IS Link	No
Patient ID	PID-3.1	Patient ID (Internal...		No		
Patient Location POC	PV1-3.1	Assigned Patient Lo...		Yes	Not Null In IS Link	No
Patient Last Name	PID-5.1	Patient Name - Fam...		Yes	Not Null In IS Link	Yes
Patient First Name	PID-5.2	Patient Name - Give...		Yes	Not Null In IS Link	Yes
Patient Middle Name	PID-5.3	Patient Name - Mid...		Yes	Not Null In IS Link	Yes
Patient Suffix	PID-5.4	Patient Name - Suffix		Yes	Not Null In IS Link	Yes
Patient Prefix	PID-5.5	Patient Name - Prefix		Yes	Not Null In IS Link	Yes
Patient Degree	PID-5.6	Patient Name - Deg...				
Patient Sex	PID-8	Sex		Yes	Not Null In IS Link	No
Patient Segment	PID-0	Pid Segment _eMS_		No		
Pre-Fetch Code	OBR-21	Filler Field 2				
Priority	OBR-27.6	Quantity/Timing - P...	Priorities Table	Yes	Not Null In IS Link	No
Procedure Code	OBR-4.1	Universal Service I...		Yes	Not Null In IS Link	No
Reading Physician ID	OBR-32.1.1	Principal Result Inte...		Yes	Not Null In IS Link	No

2. Select the row to update and click **Update Field Mapping** or select **Update Row** from the right-click menu. The configuration window appears for the chosen field.—in this example, the **Patient Last Name Configuration** window is shown.



Note: The contents of the configuration window depend on whether a dictionary table can be used, and whether the RIS Synchronization process is enabled for the chosen field.

3. In the **Mapping Source** section, you can change the HL7 field that is mapped or, if the HL7 field was previously changed, you can restore the default mapping.

    a. Click **Choose HL7 Field**.

    b. In the **Select HL7 Mapping Field** window, select the new HL7 source field to map and click **OK** to return to the configuration window.

    OR

    Click **Restore Default**.

4. To convert the HL7 value using a dictionary table, select the **Replace HL7 value using Dictionary Table** check box. Then click **Edit Table**.

    In the table that opens, edit the fields as required and click OK to return to the configuration window.

    See Section 4.6.2 Using Dictionary Tables for more information.

5. If RIS Synchronization is enabled for this field, in the **RIS-Sync Configuration** section, you can change the RIS synchronization parameters:

    a. To use RIS synchronization, select the **Enable RIS-Sync** check box.

    b. From the **Update field if** drop-down list, select the condition that defines when RIS synchronization takes place.

    c. To dicomize the RIS value during RIS synchronization, select the **Normalize RIS value** check box.

    OR

    To disable RIS synchronization, clear the **Enable RIS-Sync** check box.

6. Click **OK** to return to the configuration window.

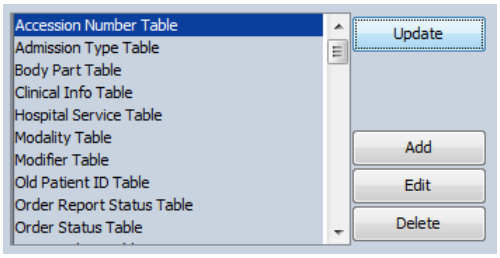
7. Click **Save**  , then restart the affected services.

4.6.2 Using Dictionary Tables

You can use simple or complex dictionary tables to convert HL7 values before they are uploaded to the IS Link database.

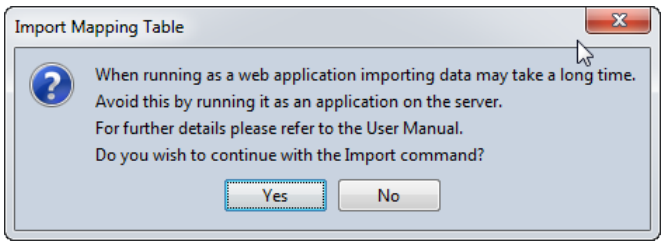
4.6.2.1 Configuring a Simple Mapping Table

1. In the left pane of the System Configuration tool, navigate to **Dictionary > Simple Mapping Tables**. The list of simple mapping tables appears in the right pane.



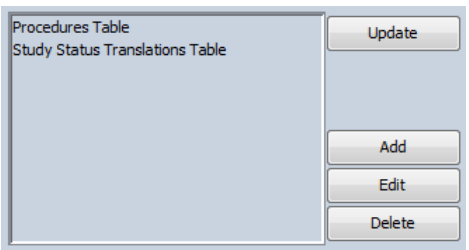
2. From here, you can do the following:

To:	Do this:
Add data	1. Select the relevant table from the list and click **Update**. 2. In the window that appears, click **Add Data**  . 3. In the **Insert Data** window, type the new value and the converted value. 4. To add more values, click **Save & Clear** and repeat step 3. 5. When you have finished adding values, click **OK**. 6. Click Exit  to close the window.
Update values	1. Select the relevant table from the list and click **Update**. 2. In the window that appears, select the values to update and click **Update Data**  . 3. In the **Update Data** window, type the relevant values and click **OK**. 4. Repeat steps 2-3 to update additional values, as required. 5. When you have finished updating values, click **OK**. 6. Click **Exit**  to close the window.
Delete a value	1. Select the relevant table from the list and click **Update**. 2. In the window that appears, click **Delete Data**  . 3. In the confirmation message that appears, click **Yes**. 4. Click **Exit**  to close the window.

To:	Do this:
Import a conversion file	1. Select the relevant table from the list and click **Update**. 2. In the window that appears, click **Import**   3. In the **Import** window, type the location of the conversion file in the **File Path** box or click **Browse** to find the location. 4. In the **Column Delimiter** box, type the delimiter used to separate the columns in the conversion file. 5. In the **Import Type** section, select whether to import new rows or overwrite data in the mapping table. 6. Click **Import** to import the conversion table. 7. When the conversion table is imported successfully, click **OK** in the message that appears. 8. Click **Exit**  to close the window.
Add a new mapping table	1. Click **Add**. 2. In the **Add Simple Mapping Table** window, type the name of the new mapping table and click **OK**. The new mapping table appears at the end of the list of simple mapping tables. See Add data for details on how to add values to the new table.
Rename a simple mapping table	1. Select the relevant table from the list and click **Edit**. 2. In the **Update Simple Mapping Table** window, type the new name of the mapping table and click **OK**.
Delete a simple mapping table	1. Select the table you want to delete and click **Delete**. 2. In the confirmation message that appears, click **Yes**.

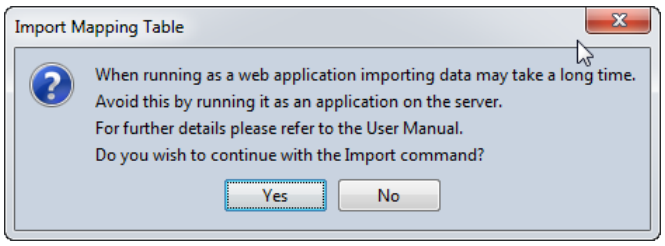
4.6.2.2 Configuring a Complex Dictionary Table

1. In the left pane of the System Configuration tool, navigate to **Dictionary > Complex Mapping Tables**. The list of complex mapping tables appears in the right pane.



2. From here, you can do the following:

To:	Do this:
Add data	1. Select the relevant table from the list and click **Update**. 2. In the window that appears, click **Add Data**  . 3. In the **Insert Data** window, type the new value and the converted value. 4. To add more values, click **Save & Clear** and repeat step 3. 5. When you have finished adding values, click **OK**. 6. Click Exit  to close the window.
Update values	1. Select the relevant table from the list and click **Update**. 2. In the window that appears, select the values to update and click **Update Data**  . 3. In the **Update Data** window, type the relevant values and click **OK**. 4. Repeat steps 2-3 to update additional values, as required. 5. When you have finished updating values, click **OK**. 6. Click **Exit**  to close the window.
Delete a value	1. Select the relevant table from the list and click **Update**. 2. In the window that appears, click **Delete Data**  . 3. In the confirmation message that appears, click **Yes**. 4. Click **Exit**  to close the window.

To:	Do this:
Import a conversion file	9. Select the relevant table from the list and click **Update**. 10. In the window that appears, click **Import**  .  11. In the **Import** window, type the location of the conversion file in the **File Path** box or click **Browse** to find the location. 12. In the **Column Delimiter** box, type the delimiter used to separate the columns in the conversion file. 13. In the **Import Type** section, select whether to import new rows or overwrite data in the mapping table. 14. Click **Import** to import the conversion table. 15. When the conversion table is imported successfully, click **OK** in the message that appears. 16. Click **Exit**  to close the window.
Add a new mapping table	3. Click **Add**. 4. In the **Add Simple Mapping Table** window, type the name of the new mapping table and click **OK**. The new mapping table appears at the end of the list of simple mapping tables. See Add data for details on how to add values to the new table.
Rename a simple mapping table	3. Select the relevant table from the list and click **Edit**. 4. In the **Update Simple Mapping Table** window, type the new name of the mapping table and click **OK**.
Delete a simple mapping table	3. Select the table you want to delete and click **Delete**. 4. In the confirmation message that appears, click **Yes**.

4.7 Configuring the Info Router

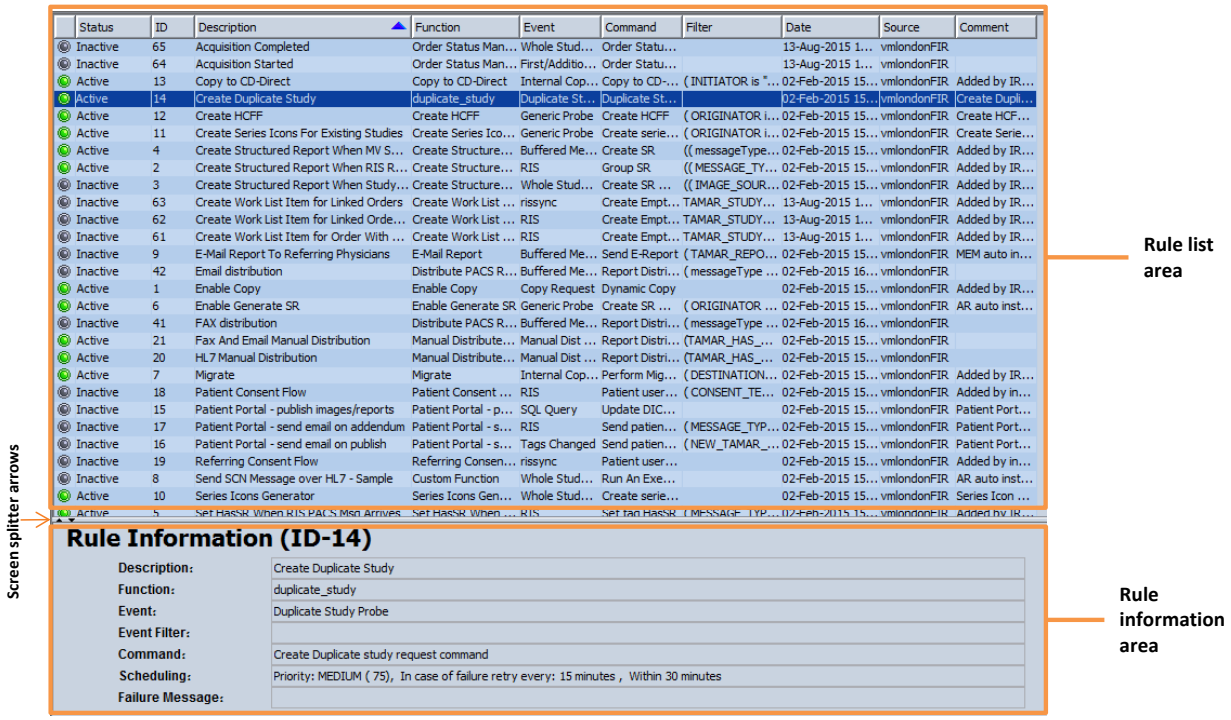
The Info Router provides flexible and rule-driven data management and auto-forwarding capabilities.

You can use the System Configuration tool to configure Info Router rules for archiving new data, burning CDs, pre-fetching data from within or outside CARESTREAM Vue PACS, synchronizing Workflow Manager metadata across sites, and many other data management activities.

An Info Router rule includes:

- An *event*—Provides the trigger for the Info Router. Examples include the arrival of a new image, study, or report.
- A *command*—Defines the actions that the Info Router performs after being triggered by an event. For example, move DICOM data, send tag updates, and send HL7 messages. Commands can be grouped and can also have an *alias*. An alias is an alternative target for a command (such as a person or a device), with its own set of rules. For example, copy the DICOM study to Dr. Smith, except on Sundays, when it is copied to Dr. Jones instead.
- A *filter*—Events can be filtered, for example, so only new CT images trigger the Info Router.

Info Router rules are displayed in a table, as shown in the following figure.



The Rule List area, in the upper pane, displays a list of the rules that are defined for the system, together with general information and the current status of each rule.

When you select a rule, the rule details appear in the Rule Information area, in the lower pane.

You can use the screen splitter arrows between the areas to resize the Rule Information area, or click and drag it to a new position.

4.7.1 Configuring Info Router Rules

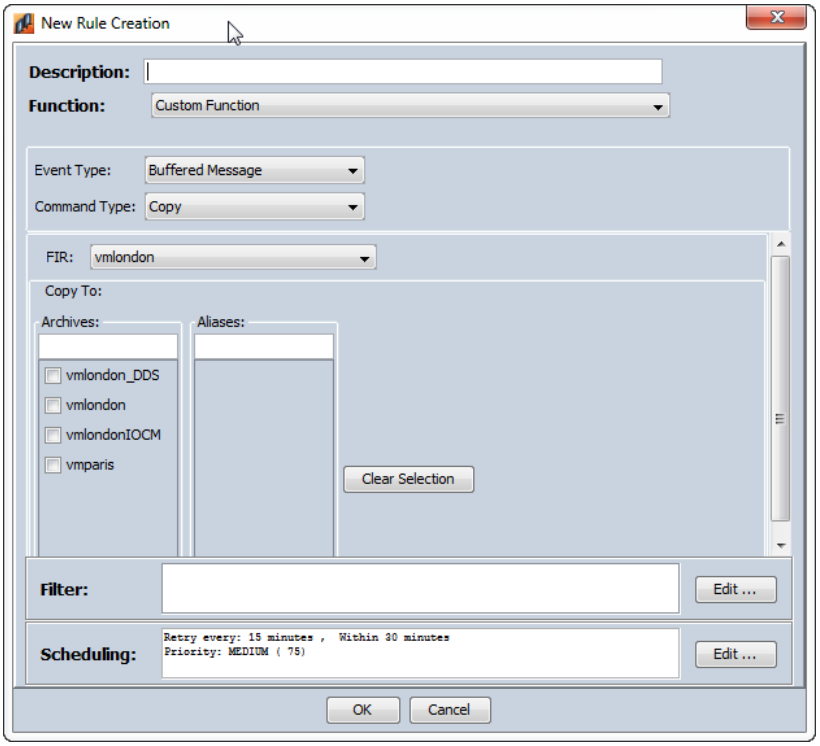
You use the System Configuration tool to configure Info Router rules, as follows:

- Using predefined functions, which are packaged combinations of events, filters, and commands. Examples include:
  - Backup
  - Copy images/studies
  - Create structured reports
  - Burn and copy
  - Pre-fetch/Pre-load
  - Update tags
  - Synchronize tags between Workflow Managers
- Using custom functions that include a combination of events, filters, and commands not provided by the predefined functions.

4.7.1.1 Adding an Info Router Rule using Predefined Functions

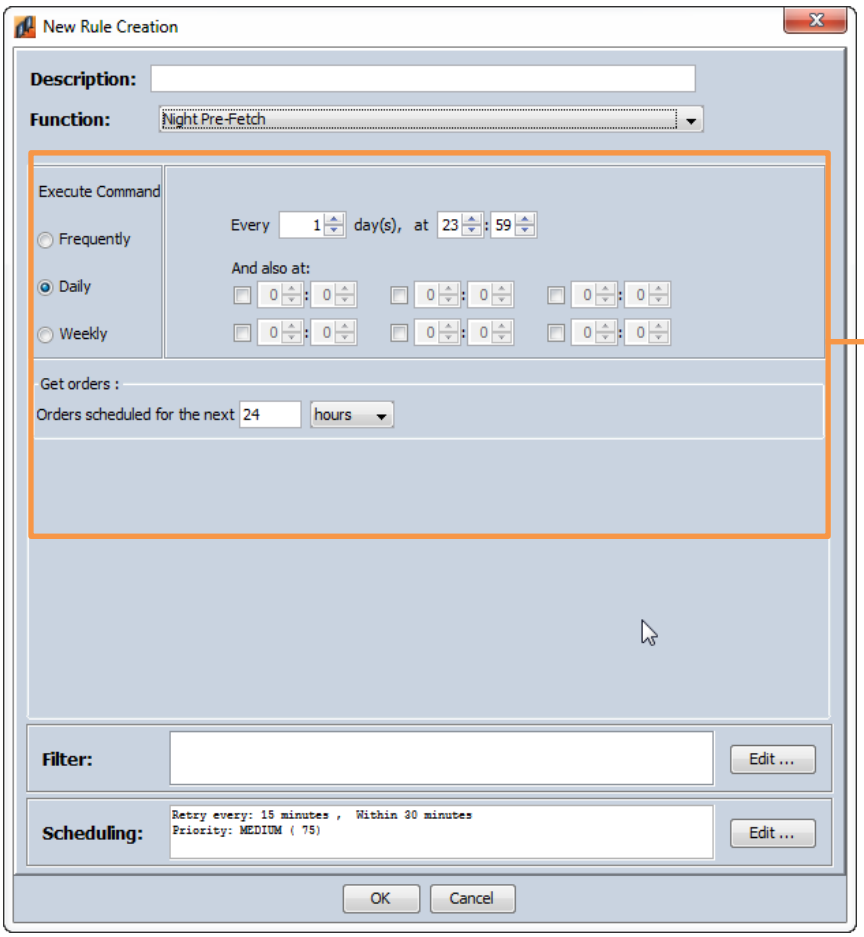
1. In the left pane of the System Configuration tool, navigate to **Info-Router > Rules**. The rule display area appears in the right pane.
2. To add a rule, do one of the following:
   - From the System Configuration toolbar, click **Add** 
   - Select **Add** from the right-click menu.
   - Right-click the list rule area and select **Insert Rule**.

   The **New Rule Creation** window appears.



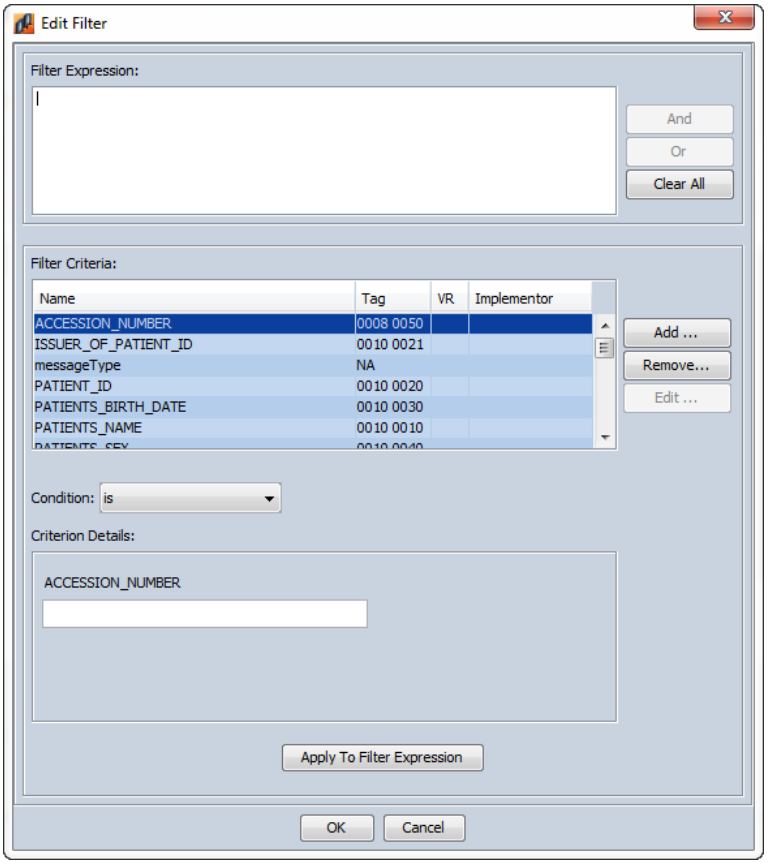
3. In the **Description** box, type a description of the rule.
4. From the **Function** drop-down list, select a pre-defined function. The parameters section changes depending on the function selected.

   In this example, the Night Pre-Fetch rule is selected.



5. In the parameters section, complete the relevant parameters for the function.

6. To set an event filter, in the **Filter** section, click **Edit**. The **Edit Filter** window appears

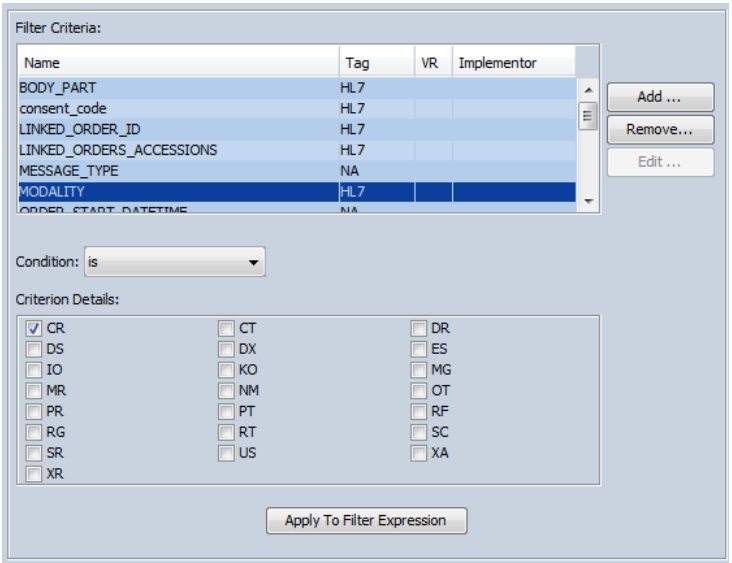


7. In the **Edit Filter** window, you compose a filter expression as follows:

   a. Select a criterion from the **Filter Criteria** list. If you do not find a suitable criterion, click **Add**, and in the **Filter Fields Editor** window, select a field and click **Add**.

      The **Criterion Details** section changes depending on the criterion selected.

      In this example, **MODALITY** is selected as the filter criterion. A list of modalities is presented in the **Criterion Details** section.



b. Select a condition from the **Condition** drop-down list.

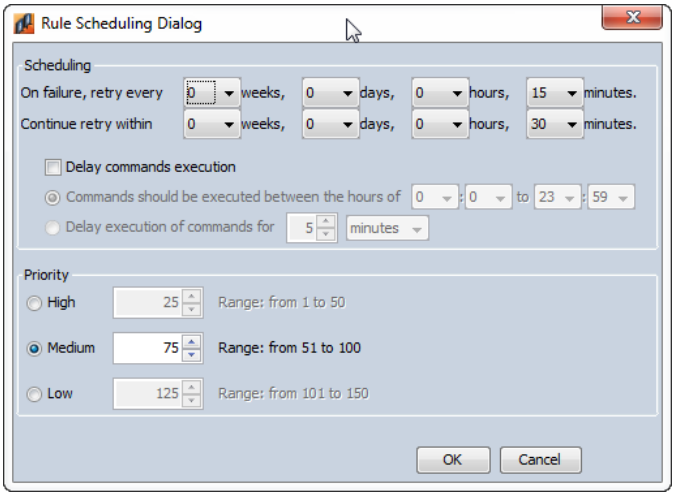
c. Select the relevant criterion details in the **Criterion Details** section.

d. Click **Apply to Filter Expression**. The filter expression appears in the **Filter Expression** section.

e. Repeat steps a-d to add additional expressions.

f. Click **OK** to return to the **New Rule Creation** window.

8. To configure rule scheduling, in the **Scheduling** section, click **Edit**. The **Rule Scheduling Dialog** window appears.



9. Use the drop-down lists and other controls to define the default scheduling parameters for the rule.

10. Click **OK** to return to the **New Rule Creation** window.

11. Click **OK** to return to the rule display area window.

4.7.1.2 Adding an Info Router Rule using Custom Functions

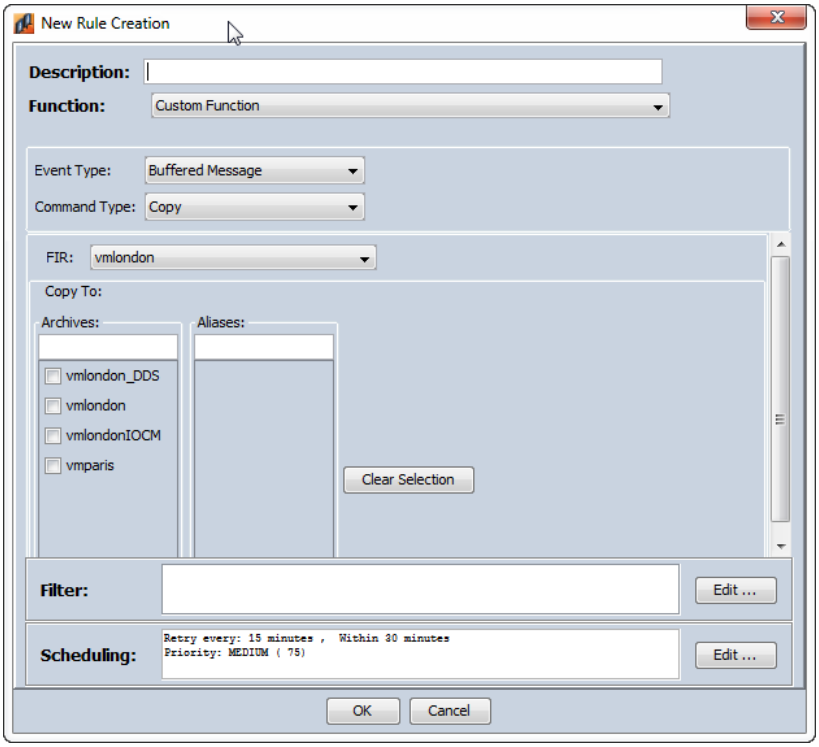
Note: It is recommended to consult with Carestream Professional Services personnel before adding or modifying Info Router rules using custom functions.

1. In the left pane of the System Configuration tool, navigate to **Info-Router > Rules**. The rule display area appears in the right pane.

2. To add a rule, do one of the following:

   - From the System Configuration toolbar, click **Add** 
   - Select **Add** from the right-click menu.
   - Right-click the list rule area and select **Insert Rule**.

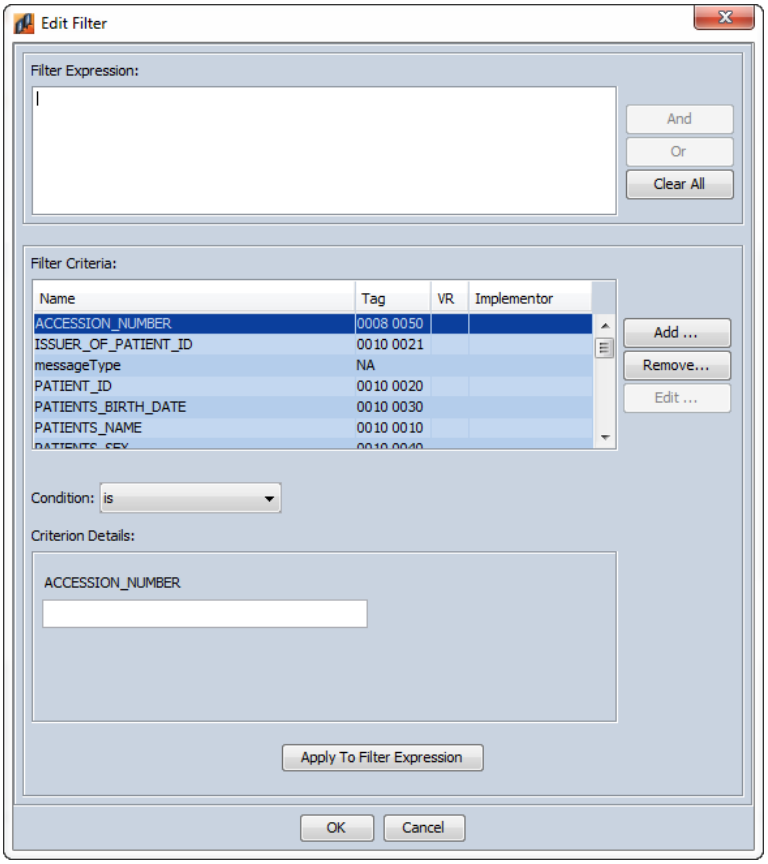
   The **New Rule Creation** window appears.



3. In the New Rule Creation window, you define the rule parameters, as follows:
   a. In the **Description** box, type a description of the rule.
   b. From the **Function** drop-down list, select **Custom Function**.
   c. From the **Event Type** drop-down list, select the relevant event type.
   d. From the **Command Type** drop-down list, select the relevant command type. To configure a group command, select **Group Command**.

      The parameters section changes depending on the event type and command type selected.
   e. In the parameters section, complete the relevant parameters for the function and add actions to the group. If required, you can define another set of group commands and specify whether these commands should be executed sequentially or in parallel.

4. To set an event filter, in the **Filter** section, click **Edit**. The **Edit Filter** window appears

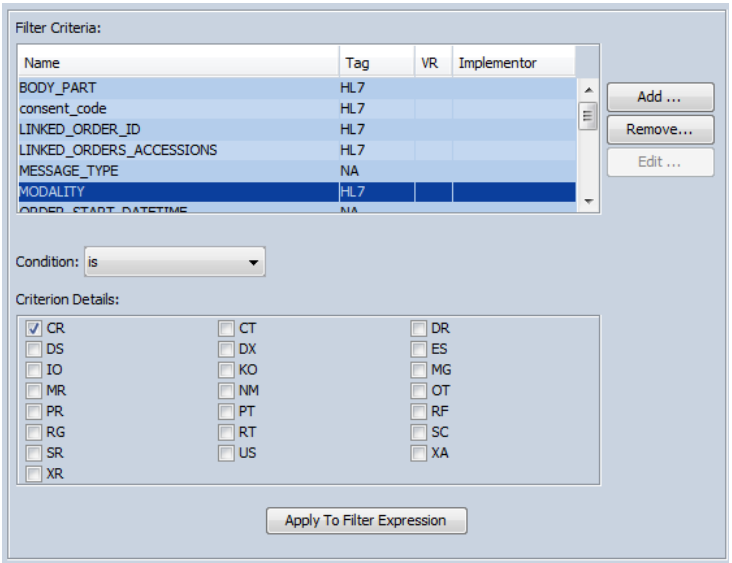


5. In the **Edit Filter** window, you compose a filter expression as follows:

   a. Select a criterion from the **Filter Criteria** list. If you do not find a suitable criterion, click **Add**, and in the **Filter Fields Editor** window, select a field and click **Add**.

      The **Criterion Details** section changes depending on the criterion selected.

      In this example, **MODALITY** is selected as the filter criterion. A list of modalities is presented in the **Criterion Details** section.



b. Select a condition from the **Condition** drop-down list.

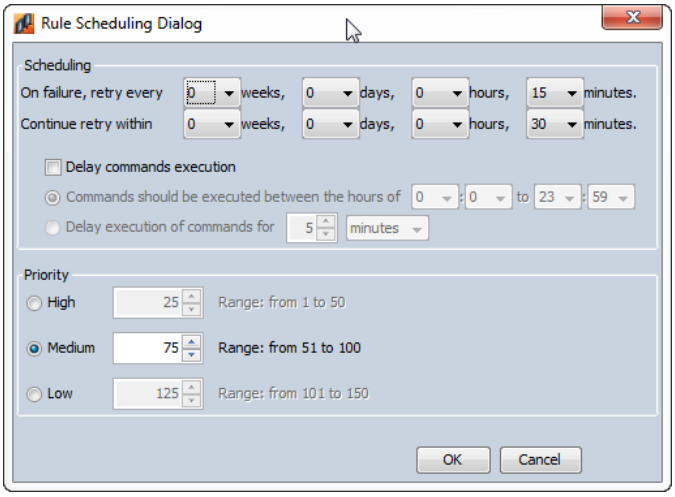
c. Select the relevant criterion details in the **Criterion Details** section.

d. Click **Apply to Filter Expression**. The filter expression appears in the **Filter Expression** section.

e. Repeat steps a-d to add additional expressions.

f. Click **OK** to return to the **New Rule Creation** window.

6. To configure rule scheduling, in the **Scheduling** section, click **Edit**. The **Rule Scheduling Dialog** window appears.



7. Use the drop-down lists and other controls to define the default scheduling parameters for the rule.

8. Click **OK** to return to the **New Rule Creation** window.

9. Click **OK** to return to the rule display area window.

4.7.1.3 Activating and Deactivating Info Router Rules

To activate or deactivate Info Router rules, select one or more rules and select **Activate**, **Deactivate**, or **Suspend** from the right-click menu.

4.7.1.4 Editing an Info Router Rule

1. In the left pane of the System Configuration tool, navigate to **Info-Router > Rules**. The rule display area appears in the right pane.

2. To edit a rule, select the rule and do one of the following:

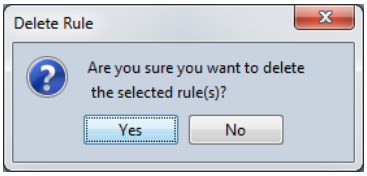
   - From the System Configuration toolbar, click **Edit** 
   - Select **Update Add** from the right-click menu.
   - Double-click the rule.

3. In the **Edit Rule** window, change the settings as required. See Section 4.7.1 Configuring Info Router Rules for more information.

4. Click **OK** to return to the rule display area.

4.7.1.5 Deleting an Info Router Rule

1. In the left pane of the System Configuration tool, navigate to **Info-Router > Rules**. The rule display area appears in the right pane.
2. Select or more rules and click **Delete**  or select **Delete** from the right-click menu.
3. In the **Delete Rule** window, click **Yes** to confirm the deletion and return to the rule display area.



4.7.2 Configuring Info Router Aliases

An alias is an alternative target for a command (such as a person or a device), with its own set of rules.

For example, you can create an alias called On-Call that consists of the user, Dr. Jones. The conditions for this alias may be a range of dates: January 1, 2003 16:00 to January 2, 2003 23:00. The system recognizes Dr. Jones as the on-call physician and routes information and images to Dr. Jones during the specified time frame (as defined by the rules).

Aliases are displayed in a table with the following information:

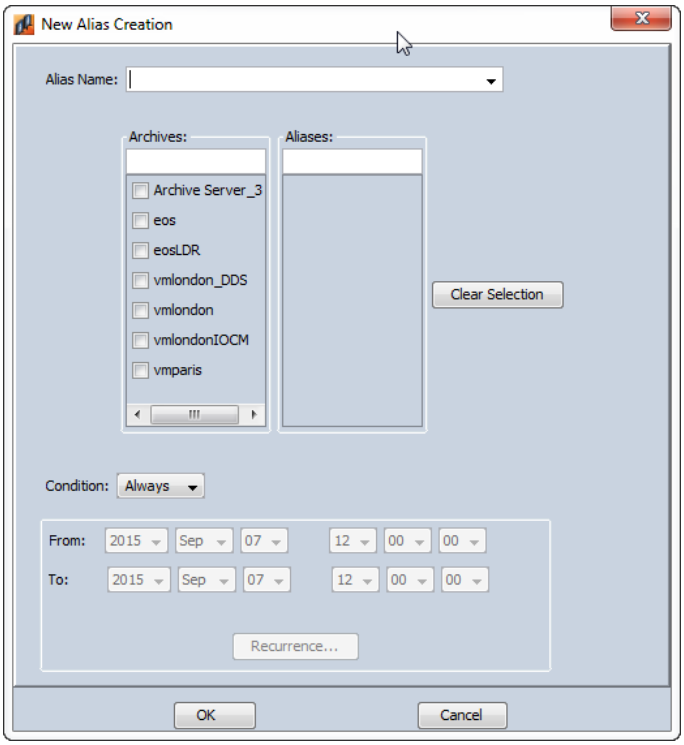
- Alias Name—The name of the alias.
- Destinations—The user or device to which the information is being copied
- Conditions—The conditions defined for the alias. Possible options are:
  - Always—Information is sent to all the items included in the alias.
  - Date—The alias is applied during a defined date range.
  - Default—Default conditions apply during dates outside of the specified date range.

You use the System Configurator to add, edit and delete Info Router aliases.

4.7.2.1 Adding an Alias

1. In the left pane of the System Configuration tool, navigate to **Info-Router > Alias**. The display area appears in the right pane.
2. From the System Configuration toolbar, click **Add**  or select **Add** from the right-click menu.

   The **New Alias Creation** window appears.



3. In the **Alias Name** box, type a name for the new alias, or select an existing alias from the drop-down list.
4. In the **Archives** area, select the archives to include in the alias.
5. In the **Aliases** area, select the existing aliases to include in the alias, if any.

   Note: Click **Clear Selection** at any time to clear the selected items.
6. From the **Condition** drop-down list, select one of the following conditions to apply to the alias:
   - Always
   - Date
   - Default
7. From the **From** and **To** drop-down lists, select the range of dates and times for which the alias is active.
8. To define a recurring alias, click **Recurrence** and, in the **Alias Recurrence** window, select the relevant days and click **OK** to return to the **Edit Alias** window.
9. Click **OK**.

   The alias appears in the display area and begins immediate operation.

   Note: To modify an existing alias, double-click the alias name in the display area to open the **Edit Alias** window.

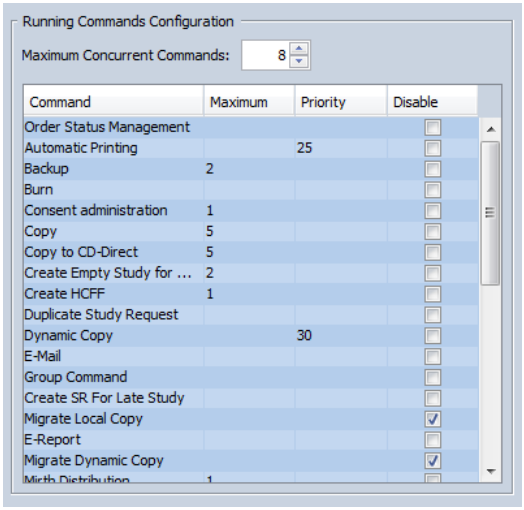
4.7.3 Configuring General Parameters

You use the System Configurator to configure general parameters that apply to all rules, such as the maximum number of commands that can run simultaneously and the priority of a command compared to other commands.

In addition, you can also define parameters that apply to specific rules, such as timeout and backup parameters.

4.7.3.1 Configuring Concurrent Commands

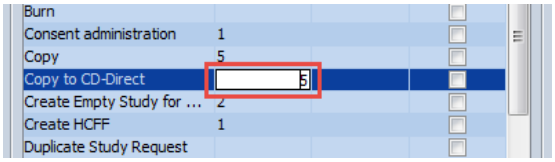
1. In the left pane of the System Configuration tool, navigate to **Info-Router > General Parameters**. The display area appears in the right pane.



2. In the **Maximum Concurrent Commands** box, enter a number or use the arrows to select the number of commands that can run simultaneously.

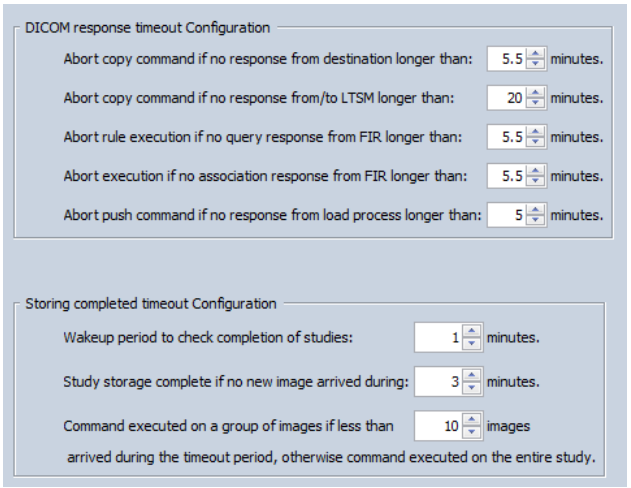
3. For each relevant command, you can define the maximum number of actions of this type that can run simultaneously and set the priority compared with other commands. The lower the number, the higher the priority. You can also disable the command, if required.

   To set the Maximum and Priority parameters, double-click the field and type the required number, as shown in the example below:



4.7.3.2 Configuring Timeout Parameters

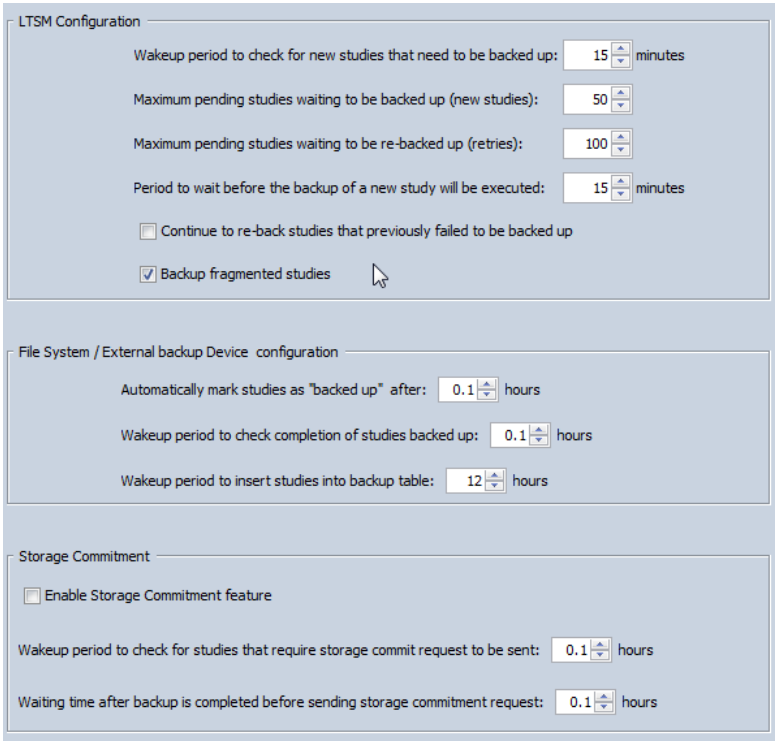
1. In the left pane of the System Configuration tool, navigate to **Info-Router > General Parameters > Timeout**. The display area appears in the right pane.



2. Complete the relevant response timeout for each of the options, as required.

4.7.3.3 Configuring Backup Parameters

1. In the left pane of the System Configuration tool, navigate to **Info-Router > General Parameters > Backup**. The display area appears in the right pane.



2. Complete the relevant backup parameters, as required.

4.8 Configuring RIS Synchronization

The RIS Synchronization process ensures that patient details in CARESTREAM Vue PACS are the same as those in RIS, and that the patient attributes stored in the Workflow Manager contain the most up-to-date details from the hospital records. If there are differences, the information from RIS is used to update the information stored in PACS.

RIS synchronization occurs whenever a study is stored in the Workflow Manager or an event takes place in RIS. RIS notifies PACS about relevant events via an HL7 interface with IS Link, which forwards the notification to the Workflow Manager.

The Workflow Manager is notified for the following events:

- A patient is added to RIS or patient details are updated – The Workflow Manager searches its database for the patient details according to the patient ID. If the patient is found, the attributes are overridden by the updated attributes in RIS.
- Patient details are merged – When two sets of details for a patient are merged in RIS, the Workflow Manager is notified. The patient details are then merged in the Workflow Manager.
- A new report is created – When a report is created in RIS, the Workflow Manager is notified. The **Has report** column in the DIDB_STUDIES table is updated to Yes. If the Workflow Manager has a related study, it updates the study status to READ. This removes studies from the UNREAD worklist that were not read using the CARESTREAM PACS Client.

- Order details are changed – When the details of an order are changed, such as the date of a scan, the Workflow Manager is notified.

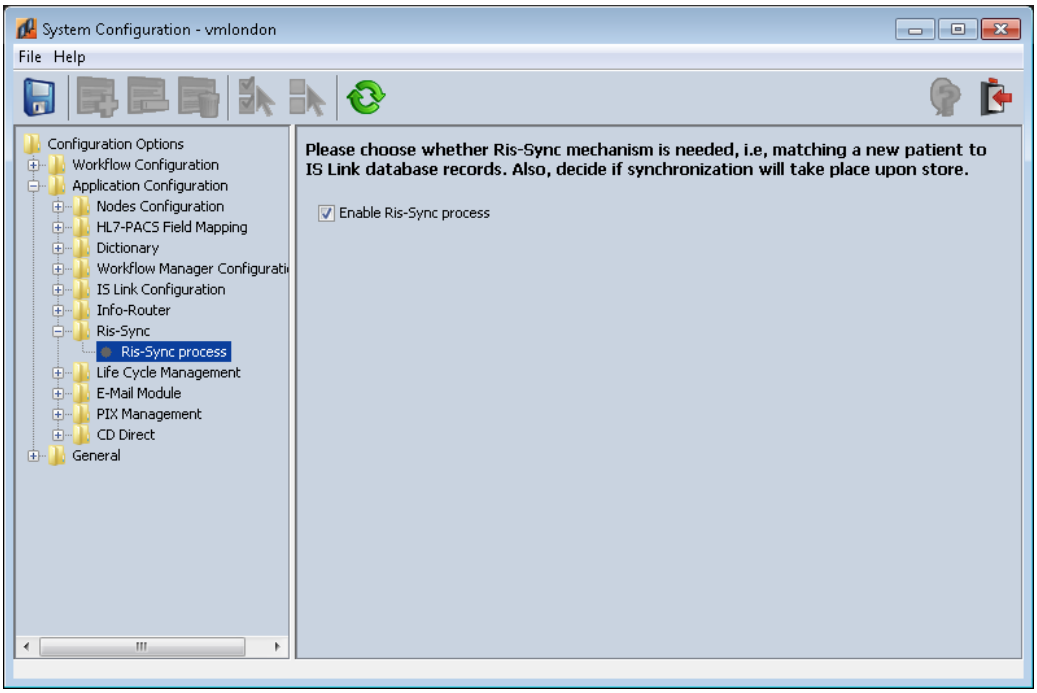
When attributes are updated as a result of the RIS Synchronization process, the old values and updated values are logged in the Audit Trail log and can be viewed using the Audit Trail Viewer.

4.8.1.1 Configuring Fields for RIS Synchronization

You use the HL7-PACS Field Mapping function to indicate which HL7 fields in RIS should be updated in the Workflow Manager. See Section 4.6 Configuring HL7-PACS Field Mapping for more information.

4.8.1.2 Enabling RIS Synchronization

1. In the left pane of the System Configuration tool, navigate to **Application Configuration > Ris-Sync > Ris-Sync process**.
2. Select the **Enable Ris-Sync process** check box in the right pane



When the RIS Synchronization process fails for some reason, it is possible to perform manual RIS synchronization. For more information, see Section 7.1.10 Performing Manual RIS Synchronization.

4.9 Configuring Life Cycle Management

Life Cycle Management provides support for the automatic transfer of images from one storage tier to another. You use the System Configuration tool to configure the rules that control the automatic migration of data across these multiple storage tiers. There is no limit to the number of storage tiers that can be used.

The migration process is a scheduled task that runs at a predefined time every day. This process queries the database for image information and evaluates the migration rules by tiers, using defined rule groups. It then uses the Info Router to migrate the actual data.

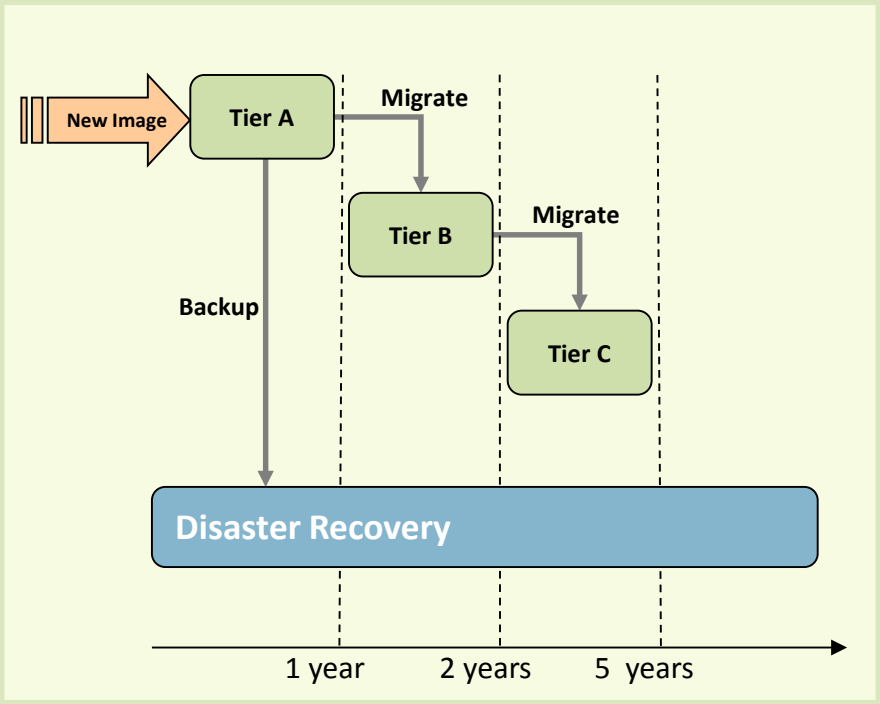
You can configure that after images are copied to the destination tier they will be deleted from the source tier. An archive tier (such as the Archive Agent) is the last tier in the life cycle. A backup process writes data to this tier immediately. The data is not deleted until the data's life cycle is complete; sometimes the data is never deleted.

The distinction between migration and backup is important to understand when configuring Life Cycle Management:

- Migration is used to migrate data from one type of media to another over time, usually as a cost/performance tradeoff.
- Backup is used to make copies of data as soon as possible after ingestion, so that images are stored on multiple media, for reliability purposes.

In this example, Life Cycle Management rules are configured as follows:

- Migrate data to Tier B after 1 year
- Migrate data to Tier C after 2 years
- Back up data to tape immediately



You can use the System Configuration tool to configure the following Life Cycle Management features:

- Image life cycle rules—Use to configure rules that define when to move images and where to move them.
- Archive settings—Use to configure server availability and the percentage storage space available for each server.
- Auto-delete priorities—Use to manage system-wide deletion rules.
- Auto-delete for database objects—Use to set the storage settings for icons.

4.9.1 Configuring Image Life Cycle Rules

You use the System Configuration tool to configure the rules that define when to move images and where to move them.

Each rule uses a rule group as a template, which defines the parameters to use when searching for images to migrate. For example, the **Study Older than [param1] days** rule group can be used to search for images that are more than a year old.

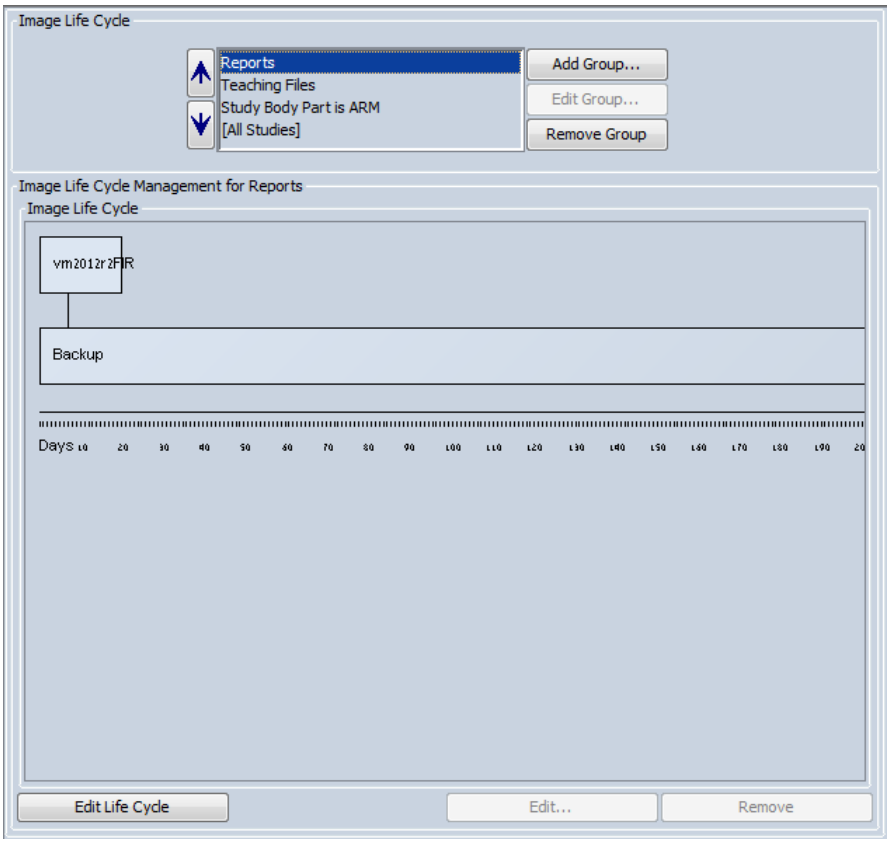
The rule groups are defined in the Central Configuration Editor in the following location:

`imaginet\system\applications\medistore\admintool\auto_delete\images\exclude_templates`

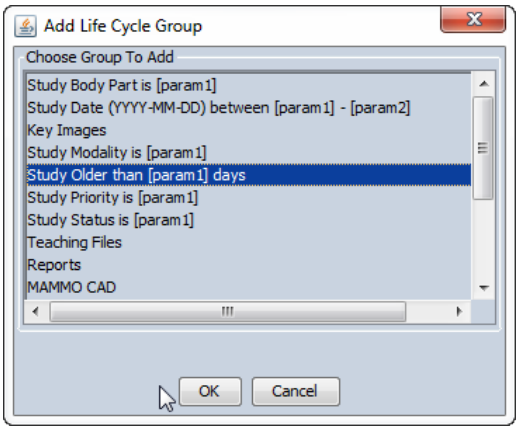
For each rule group, you define whether it is a migration (copy to new tier, then delete from old tier) or an archive (copy to new tier and leave on old tier) and when to copy the images.

4.9.1.1 Adding a Rule Group

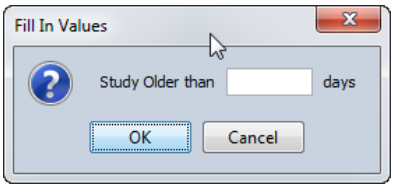
1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Life Cycle Configuration**. The configuration area appears in the right pane.



2. In the **Image Life Cycle** section, click **Add Group**.
3. In the **Add Life Cycle Group** window, select the group to add from the list of groups and click **OK**. In this example, the **Study Older than [param1] days** is selected.



4. If there is a parameter to add, type the relevant value is the **Fill In Values** window and click **OK** to return to the configuration area.



5. Use the  and  buttons to change the order of the selected rule group.

You can now configure the image life cycle for the rule group. See Section 4.9.1.4 Configuring the Image Life Cycle for details.

4.9.1.2 Updating Rule Group Parameters

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Life Cycle Configuration**. The configuration area appears in the right pane.
2. In the **Image Life Cycle** section, select the group to edit and click **Edit Group**.
3. In the **Fill In Values** window, update the value for the rule and click **OK** to return to the configuration area.

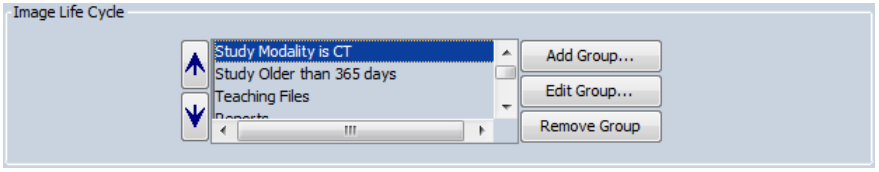
4.9.1.3 Removing a Rule Group

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Life Cycle Configuration**. The configuration area appears in the right pane.
2. In the **Image Life Cycle** section, select the group to remove and click **Remove Group**.
3. In the **Remove group** window, click **Yes** to confirm the removal and return to the configuration area.

4.9.1.4 Configuring the Image Life Cycle

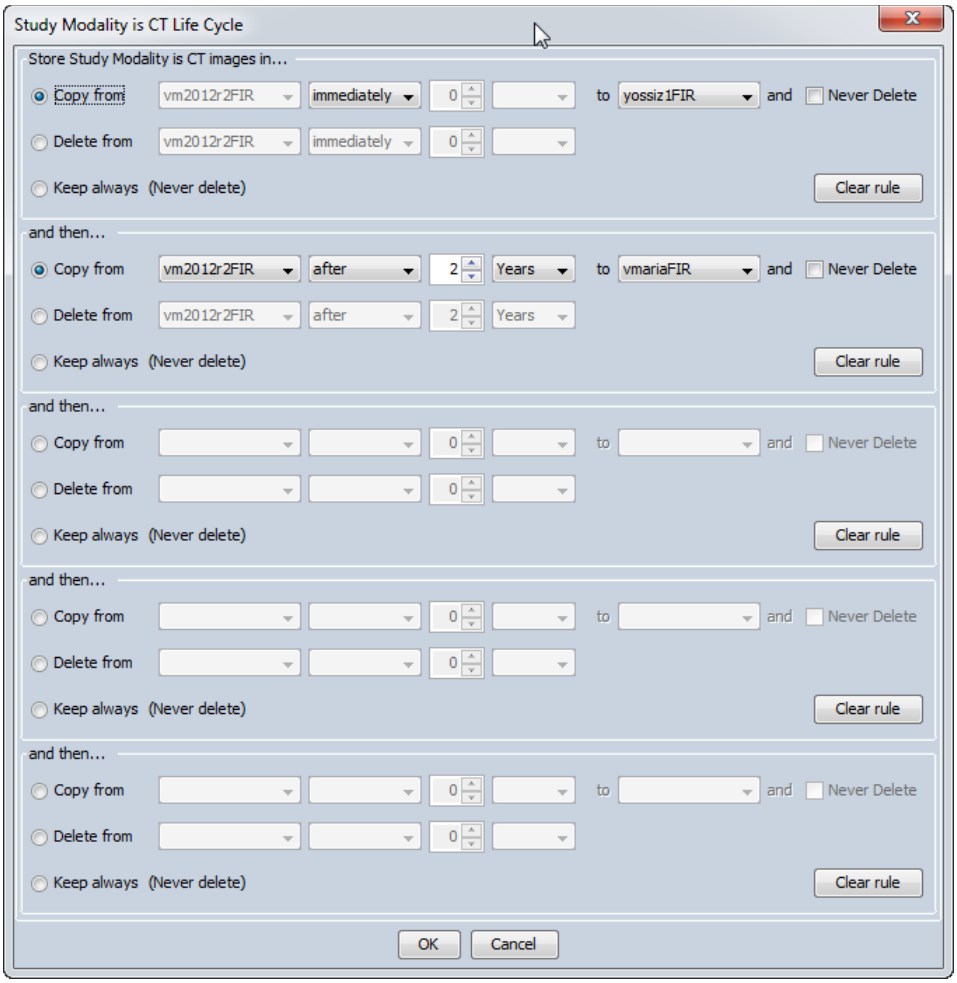
You use the **Edit Life Cycle** option to add rules to the image life cycle for a rule group and server.

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Life Cycle Configuration**.
2. In the right pane, in the **Image Life Cycle** section, select the relevant group. In this example, the **Study Modality is CT** group is selected.

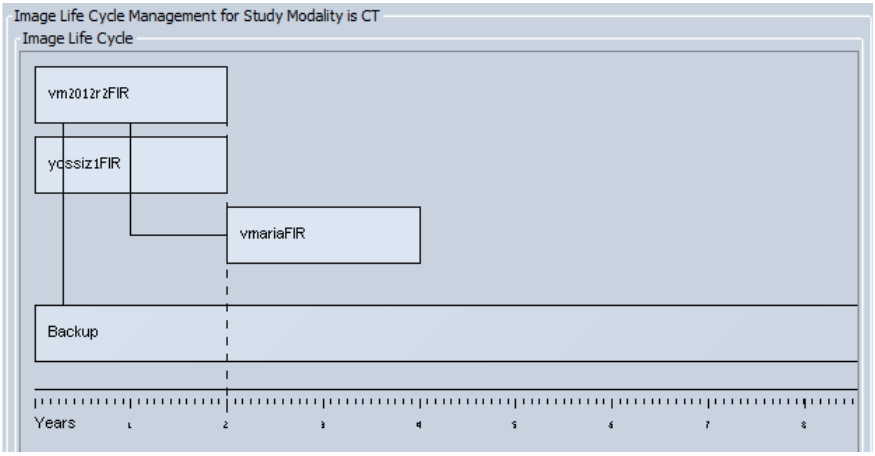


3. In the lower section, select the relevant server and click **Edit Life Cycle**.
4. In the **Life Cycle** window, use the drop-down menus to define where to copy images from and to, when to copy the images, and whether to delete from the source tier for the selected server.

   In the following example, 2 rules are defined: one to copy images immediately and one to copy images after 2 years.



5. Click **OK**. A schematic diagram of the life cycle rules appears in the lower section.



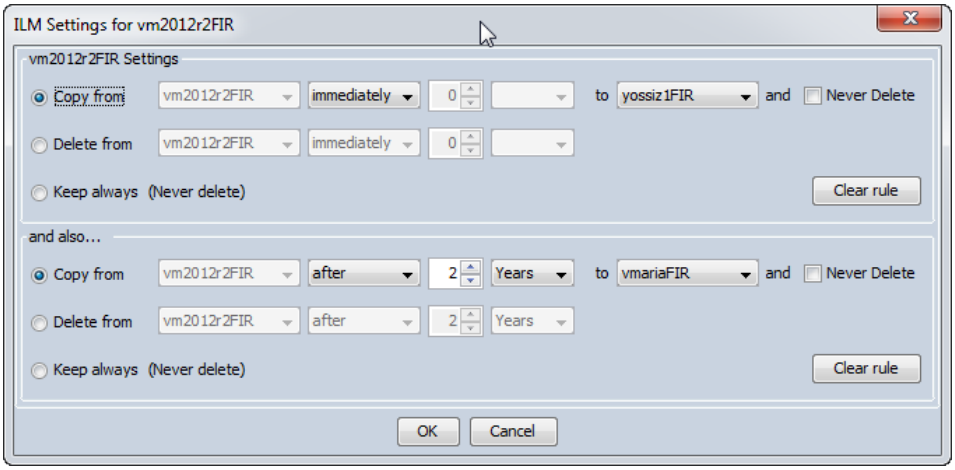
6. Repeat steps 2-5 to configure rules for additional rule groups and servers.

4.9.1.5 Updating Image Life Cycle Rules

When you have configured the image life cycle for a rule group and server, you use the **Edit** and **Remove** options to change and remove the rules.

To edit a rule:

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Life Cycle Configuration**.
2. In the right pane, in the **Image Life Cycle** section, select the rule group.
3. In the lower section, select the relevant server and click **Edit**. The **Settings** window appears for the selected rule group and server.



4. Use the drop-down menus to define where to copy images from and to, when to copy the images, and whether to delete from the source tier for the selected server.
5. Click **OK** to return to the configuration area.

To remove a rule:

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Life Cycle Configuration**.
2. In the right pane, in the **Image Life Cycle** section, select the rule group.
3. In the lower section, select the relevant server and click **Remove**. The rules for the relevant server are removed and schematic diagram is updated.

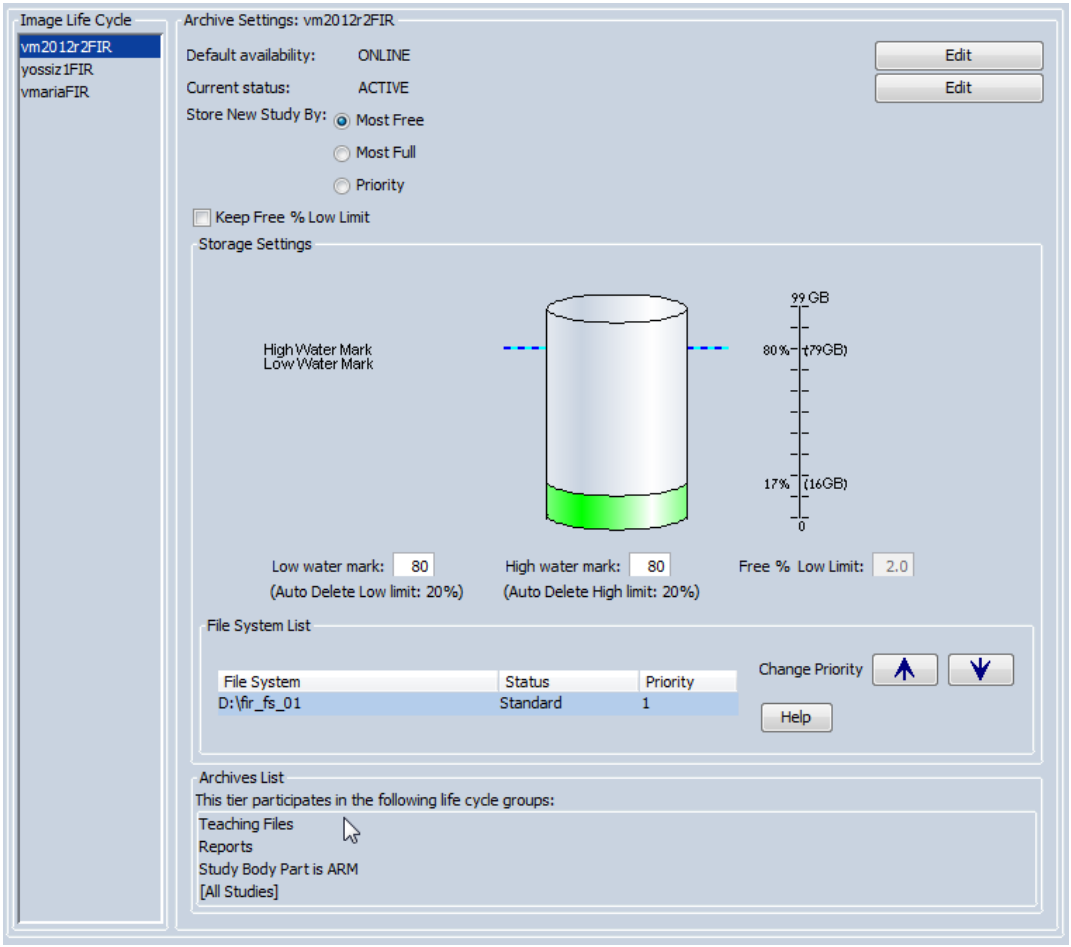
Note: If you select the main server, in this example, vm2012r2FIR, then a confirmation message appears. Click **Yes** to confirm removal of all the image life cycle rules for that server.

4.9.2 Configuring the Archive Settings

You use the System Configuration tool to configure the archive settings, which define the server availability and percentage storage space available for each server.

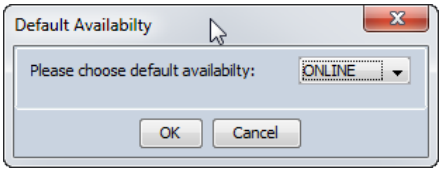
Each file-oriented storage tier is configured with a high water mark and a low water mark. In the out-of-the-box implementation, the default auto delete threshold for the main archive is set to 80%. This is the standard setting and **should not be changed**.

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Archive Configuration**. The archive settings display area appears in the right pane.



   The archive settings display area shows the storage available for the selected server, as well as other statistics. The information is displayed in cylindrical format and shows the high and low water mark levels for storage space.

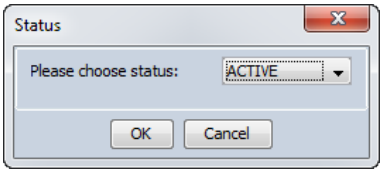
2. To view the details of different servers, select the server name in the **Image Life Cycle** section.
3. To configure the image and study availability for the selected server, click the upper **Edit** button.
4. In the **Default Availability** window, select the image and study availability from the drop-down list.



You can choose from the following options:

- ONLINE—Images are electronically accessible with high performance, as needed. This generally applies to various types of spinning storage, such as DASD, RAID, and NAS. At least one tier must be defined to provide online image availability.
- NEARLINE—Images are electronically accessible, however not with performance that users may demand. This generally applies to tape library storage (via Archive Agent) and to some DICOM or HSM storage tiers.
- NEARLINE1— Images are electronically accessible; performance is not as good as online, but it better than NEARLINE. This generally applies to CENTERA storage.
- AUTO— For the LTSM server, the status is automatically updated between NEARLINE and OFFLINE depending on whether the tape is in or out of the tape library
- OFFLINE—Images are managed from a tape library and need manual intervention for retrieval. Access performance is uncertain and can be expected to be very slow.

5. To configure the tier status for each server, click the lower **Edit** button.
6. In the **Status** window, select the tier status from the drop-down list.



You can choose from the following options:

- ACTIVE—The normal status of a tier. Data can be migrated to and from active tiers.
- READ-ONLY— Data can be accessed from a read only tier, however, data cannot be written to the tier or migrated to another tier. This status prevents a tier from participating in migration activities from the time the status is set to read-only.
- OBSOLETE—New data cannot be stored on the tier, but old data can be migrated to an active tier. This can be useful for tiers whose storage technology is obsolete and which can be emptied slowly, over time.
- UNAVAILABLE—There is a problem with the tier and it cannot be accessed.

4.9.3 Configuring Auto Delete Rules

Since there is a finite amount of disk space on the servers, space must be cleared periodically by removing those studies that are least likely to be required. You use the System Configuration tool to configure rules for removing studies.

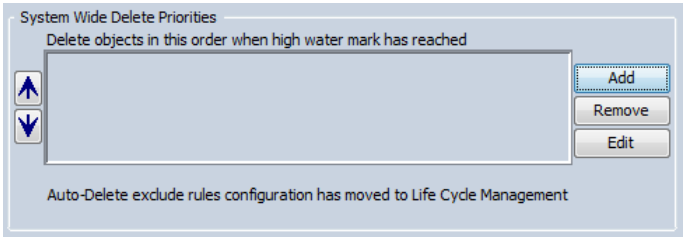
The Auto Delete process is a scheduled task that runs rules to determine the priority for deleting images from the file system. Then, when the high watermark is reached, the delete queue is processed to delete the files in this order until the low water mark is reached. Typical rules delete the oldest data first, but only if the data has been backed up.

The Auto Delete process applies to all caches on all storage tiers, as well as caches within Archive Agent.

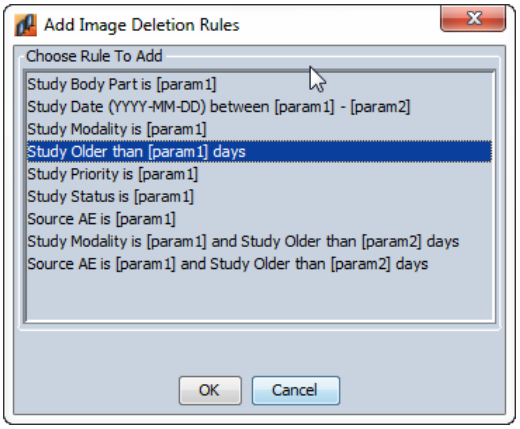
If the watermarks are not defined in the Archive Settings window, the default watermark amounts are taken from the figures configured in the Database Objects Auto Delete window.

4.9.3.1 Adding an Auto Delete Rule

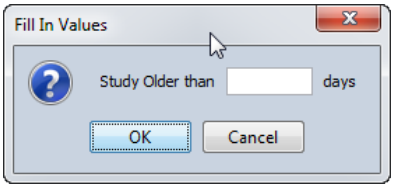
1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Auto-Delete Priorities**. The rule display area appears in the right pane.



2. To add a rule, click **Add**.
3. In the **Add Image Deletion Rules** window, select the rule to add and click **OK**. In this example, the **Study Older than [param1] days** is selected



4. If there is a parameter to add, type the relevant value is the **Fill In Values** window and click **OK** to return to the configuration area.



5. Repeat steps 2-4 to configure additional rules.
6. Use the  and  buttons to change the order of the rules.

4.9.3.2 Removing an Auto Delete Rule

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Auto-Delete Priorities**. The rule display area appears in the right pane.
2. Select the rule to remove and click **Remove**.
3. In the **Remove Rule** window, click **Yes** to confirm the removal and return to the configuration area.

4.9.3.3 Updating Auto Delete Rule Parameters

1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > Auto-Delete Priorities**. The rule display area appears in the right pane.
2. Select the rule to edit and click **Edit**.
3. In the **Fill In Values** window, update the value for the rule and click **OK** to return to the configuration area.

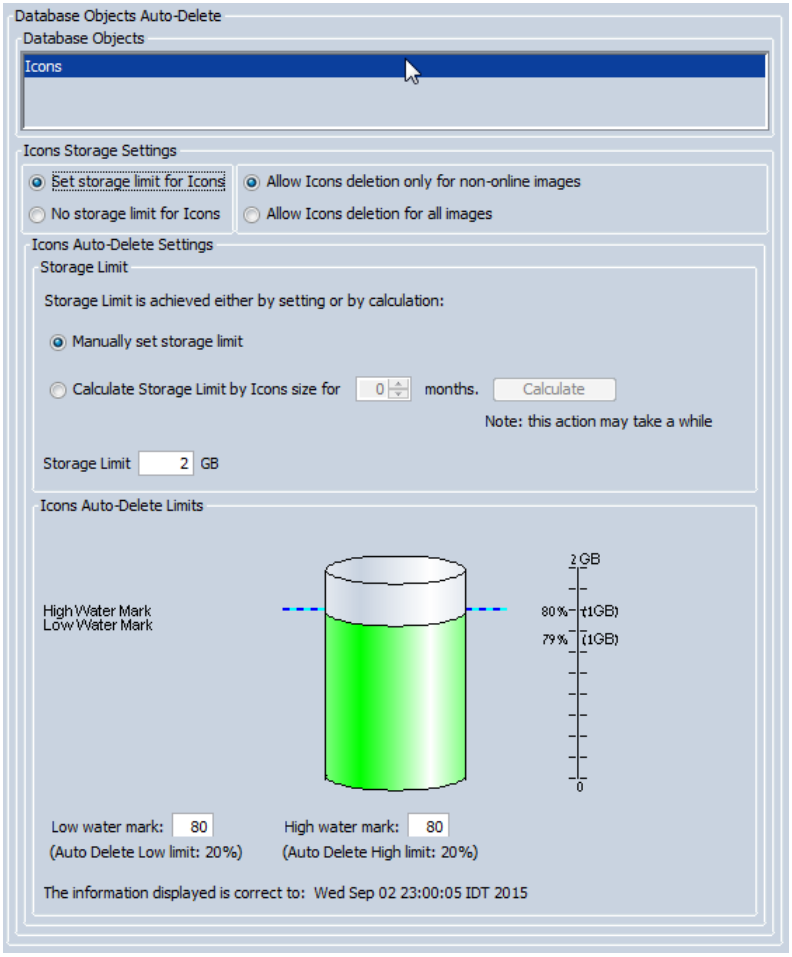
4.9.4 Configuring Auto-Delete Rules for Database Objects

Images saved as icons can be deleted based on storage availability, or after a configurable amount of time. You use the System Configuration tool to configure rules for removing these icons.

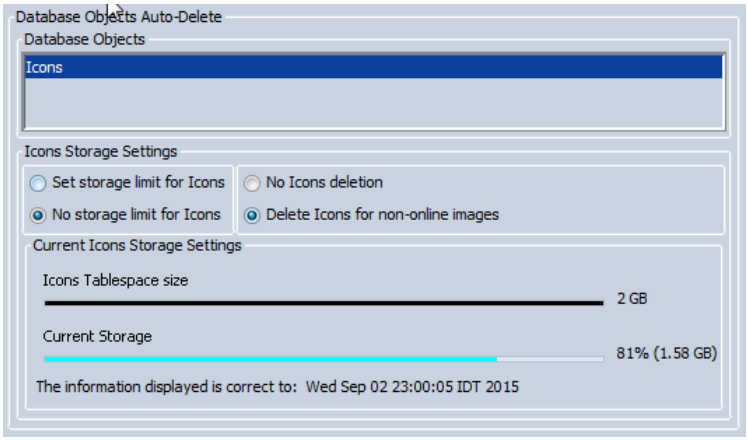
1. In the left pane of the System Configuration tool, navigate to **Life Cycle Management > DB Objects Auto-Delete**. The display area appears in the right pane.
2. In the **Icons Storage Settings** section, select from the following options:
   - **Set storage limit for Icons**—The screen expands to display the **Icons Auto-Delete Settings** section. You can specify whether to allow icon deletion for non-online images only or for all images.

     You can also manually set the storage limit or allow the system to calculate the storage limit by icon size based on the number of months entered.

     It is recommended to set the storage limit to 2 GB.



- **No storage limit for Icons**— You can specify whether to allow icon deletion for non-online images only or no icon deletion. The storage information for icons tablespace size and current storage used is displayed in linear format.



4.10 Configuring Patient Matching Rules

You use patient matching rules to define which patient attributes are matched when incoming studies are archived. This is useful, for example, to correct errors when the wrong patient ID is entered manually by technicians.

The out-of-the-box implementation includes the following default patient matching rules:

- Rule 1—based on patient ID, original patient ID, accession number
- Rule 2—based on patient ID, original patient ID, last name

You can modify the default rules or add additional rules, as required.

The patient matching mechanism runs the rules according to their priority, as follows:

Run the first rule:

If a match is found, the study is associated with the existing patient and the mechanism stops.

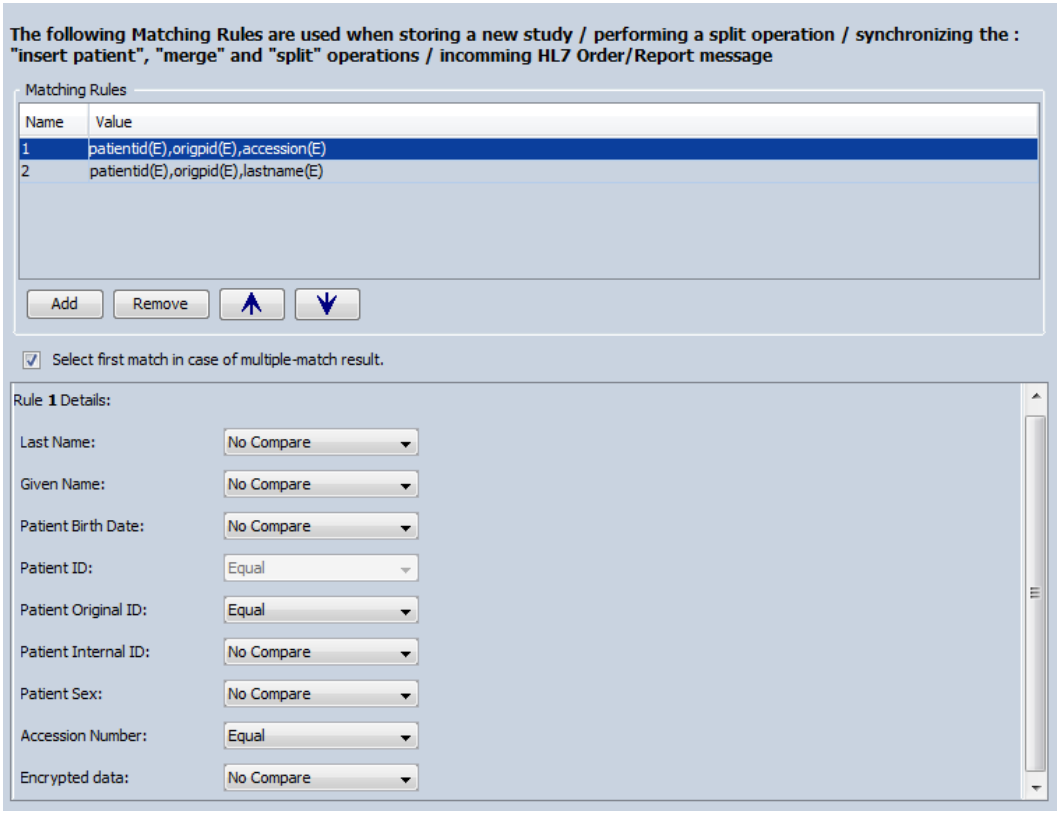
If no match is found, continue to the remaining rules until a match is found.

If no match is found:

The study is archived under a new patient ID.

4.10.1 Adding a Patient Matching Rule

1. In the left pane of the System Configuration tool, navigate to **PIX Management > Patient Management** and select **onstore**. The rule display area appears in the right pane.



2. Click **Add**. The new rule appears in the rule display area.
3. Select the **Select first match in case of multiple-match result** check box, if required.
4. In the **Rule Details** section, configure the patient matching criteria for each of the relevant attributes. Choose from the following options:
    - No Compare—the attributes are not compared
    - Equal or NULL—the attributes must be equal or empty to match
    - Equal—the attributes must be equal to match
    - Equal Non Empty—the attributes must be equal and not empty to match
5. Repeat steps 2-4 to add additional patient matching rules.
6. Use the  and  buttons to change the order of the selected rules.
7. Click Save  .

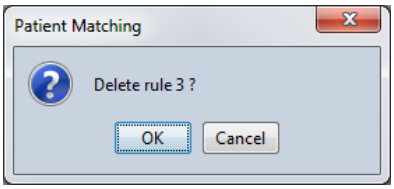
4.10.2 Editing a Patient Matching Rule

1. In the left pane of the System Configuration tool, navigate to **PIX Management > Patient Management** and select **onstore**. The rule display area appears in the right pane.
2. Select the rule you want to edit.

3. In the **Rule Details** section, modify the patient matching criteria for the rule. See Section 4.10.1 Adding a Patient Matching Rule for more information on possible options.
4. Click Save  .

4.10.3 Deleting a Patient Matching Rule

1. In the left pane of the System Configuration tool, navigate to **PIX Management > Patient Management** and select **onstore**. The rule display area appears in the right pane.
2. Select the relevant rule and click **Remove**.
3. In the Patient Matching window, click **Yes** to confirm the deletion and return to the rule display area.



4. Click Save  .

5 Performing System Monitoring Tasks

You can use System Monitoring tools to perform system monitoring tasks, including:

- Performing System Checks
- Using the Info Router
- Using the Audit Trail Viewer
- Using the Synchronization Monitor
- Comparing Archives

5.1 Performing System Checks

You can use the System Monitoring & Control tool to monitor processes and run system checks. You can do the following:

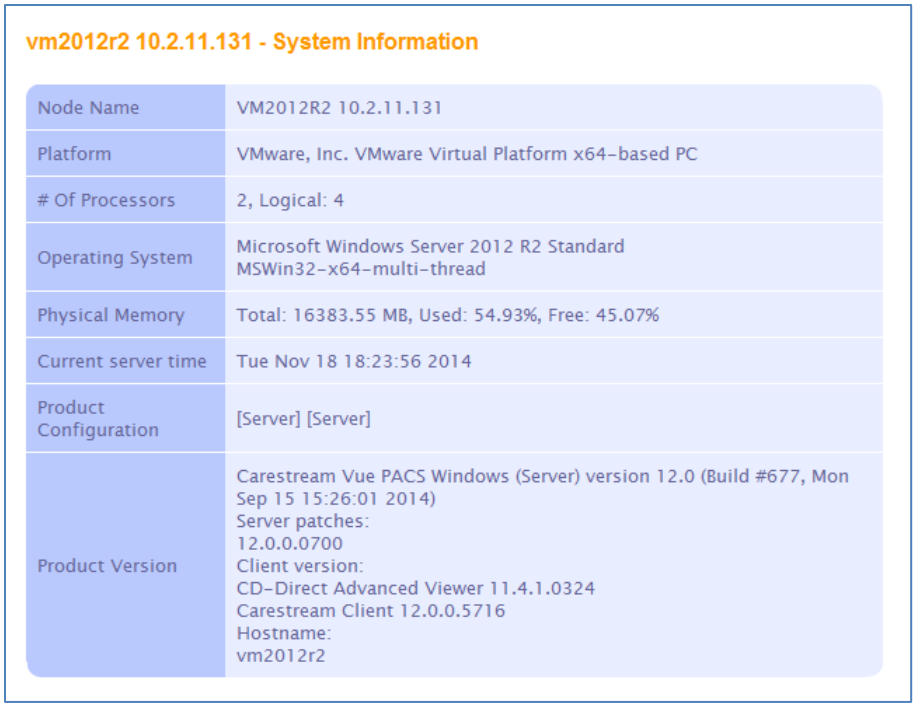
- View system information
- Check the status of licenses
- Run system checks
- Monitor server processes
- Monitor MVS processes
- Run bandwidth tests
- View the Info Router status

To open the System Monitoring & Control tool, select **System Monitor > System Check** from the Administration Tool menu. The System Monitoring & Control tool opens showing links in the left pane.

Note: The System Monitoring & Control tool is not available in cluster server deployments.

5.1.1 Viewing System Information

In the left pane, click the **System Information** link to view general system and product information.

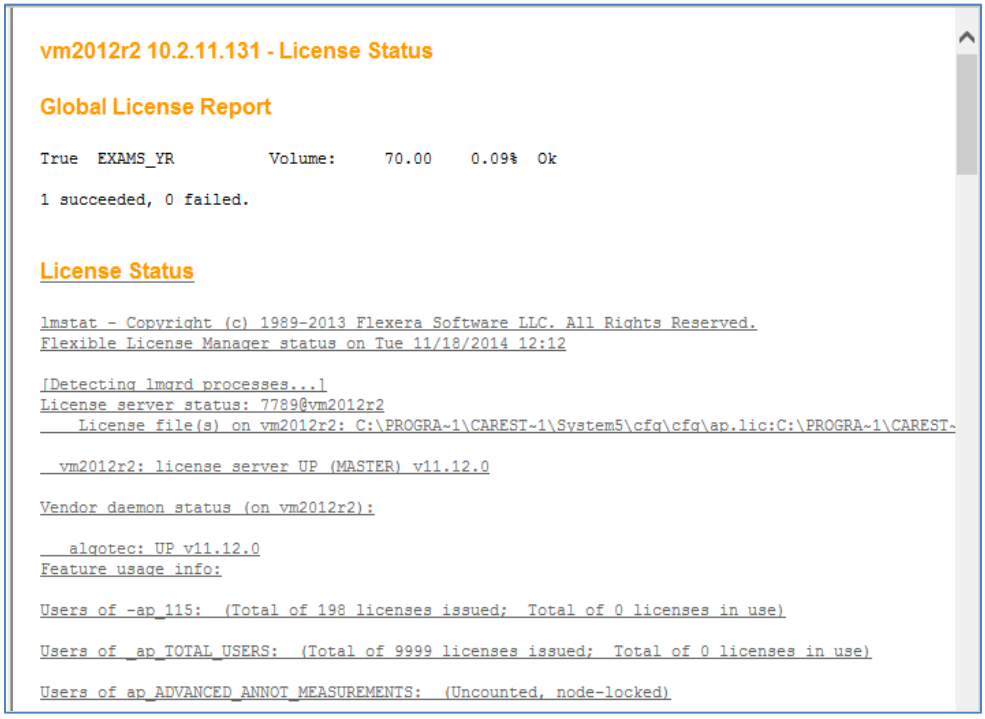


vm2012r2 10.2.11.131 - System Information

Node Name	VM2012R2 10.2.11.131
Platform	VMware, Inc. VMware Virtual Platform x64-based PC
# Of Processors	2, Logical: 4
Operating System	Microsoft Windows Server 2012 R2 Standard MSWin32-x64-multi-thread
Physical Memory	Total: 16383.55 MB, Used: 54.93%, Free: 45.07%
Current server time	Tue Nov 18 18:23:56 2014
Product Configuration	[Server] [Server]
Product Version	Carestream Vue PACS Windows (Server) version 12.0 (Build #677, Mon Sep 15 15:26:01 2014) Server patches: 12.0.0.0700 Client version: CD-Direct Advanced Viewer 11.4.1.0324 Carestream Client 12.0.0.5716 Hostname: vm2012r2

5.1.2 Checking the License Status

In the left pane, click the **License Status** link to view the global license report and license status for a server. The license status shows the number of licenses issued and the number of licenses in use.



vm2012r2 10.2.11.131 - License Status

Global License Report

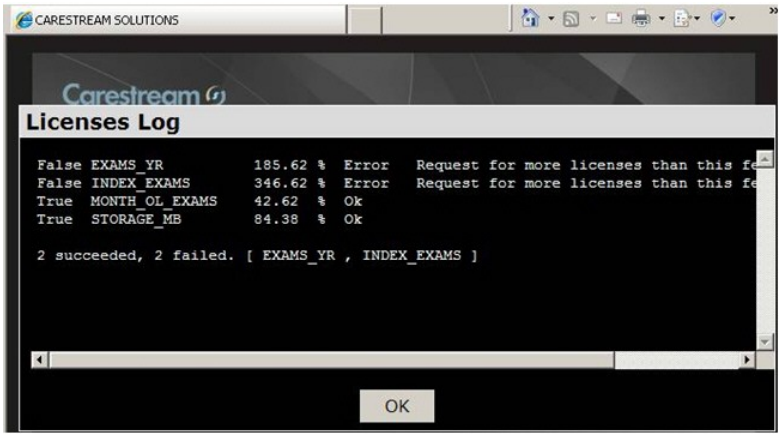
```
True  EXAMS_YR          Volume:     70.00    0.09%  Ok

1 succeeded, 0 failed.
```

License Status

```
lmstat - Copyright (c) 1989-2013 Flexera Software LLC. All Rights Reserved.
Flexible License Manager status on Tue 11/18/2014 12:12

[Detecting lmgrd processes...]
License server status: 7789@vm2012r2
    License file(s) on vm2012r2: C:\PROGRA~1\CAREST~1\System5\cfg\cfg\ap.lic:C:\PROGRA~1\CAREST~

  vm2012r2: license server UP (MASTER) v11.12.0

Vendor daemon status (on vm2012r2):

   algotec: UP v11.12.0
Feature usage info:

Users of -ap_115:  (Total of 198 licenses issued;  Total of 0 licenses in use)

Users of _ap_TOTAL_USERS:  (Total of 9999 licenses issued;  Total of 0 licenses in use)

Users of ap_ADVANCED_ANNOT_MEASUREMENTS:  (Uncounted, node-locked)
```

When a license violation occurs, a warning notification appears on the Administration Tool home page.

Click the warning notification to display the Licenses Log, which details the license errors.



Each line in the log indicates whether there is a violation (or error in the check). The percentage values quantify the amount of violation from the licensed amount.

IMPORTANT: The license violation **does not interfere** with system operation. You **must** contact a Carestream representative to check or renew the license.

5.1.3 Running System Checks

The system automatically performs a number of system checks, including network, server resources, and database checks. You can view the status of these checks and run specific checks again. You can also deactivate or reactivate any of the system checks.

In the left pane, click the Run System Check link to view the system checks in table format. Click the column name to sort the table by that column.

5.1.3.1 Run System Check Window Elements

Element	Type	Description
Check All	Button	Click to run all checks immediately. To view the results, click View All or View Errors after a few minutes.
View All	Button	Click to view the check results.
View Errors	Button	Click to view errors or warning. Each column can be sorted by pressing the column header.
Status	Column	The status of the check. Possible values are: • Green – OK • Red – Error • Yellow – Warning • Gray – Inactive
Category	Column	The type of check. Possible values are: • app • db • network • ltsm • system
Name	Column	The name of the check.
Details	Column	The details of the check.
Check Time	Column	The time the check was made.
Log	Hyperlink	Click to view the log and history of errors of the specific check.
Run	Hyperlink	Click to run the check again. The page is automatically refreshed when the check finishes running.
Repair	Hyperlink	For scripts that have a repair action, click the link to repair errors. The page is automatically refreshed when the repair finishes running.

Element	Type	Description
Deactivate/Activate	Hyperlink	Click to disable or enable a specific check. When you click Deactivate, the link text changes to Activate and the status changes to inactive.

5.1.4 Monitoring Server Processes

You can monitor the server processes that are running and start and stop specific processes.

In the left pane, click the **Server Processes** link to view the system processes that are running. The system processes are displayed in table format. Click the column name to sort the table by that column.

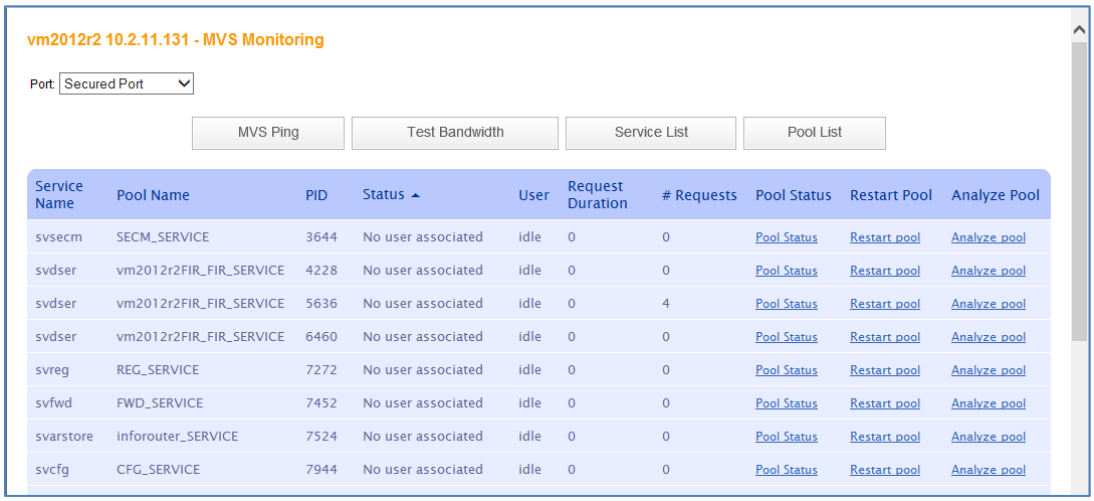
5.1.4.1 Server Processes Window Elements

Element	Type	Description
Status	Column	The status of the process. Possible values are: • Green – Running • Red – Stopped • Gray – Inactive
Process	Column	The name of the check.
PID	Column	The process ID number.
#	Column	The number of processes currently running.
CPU Time	Column	The total CPU time the process used.
Memory (M)	Column	The total real memory the process used.
Max Memory (M)	Column	The maximum amount of memory the process can use. If the process exceeds the memory limit, it is automatically restarted.
Stop	Hyperlink	Click to stop the process.
Start	Hyperlink	Click to start the process.
Deactivate/Activate	Hyperlink	Click to disable or enable a specific process. When you click Deactivate, the link text changes to Activate and the status changes to deactivated. When the process is deactivated, it is not automatically restarted.

5.1.5 Monitoring MVS Services

You can view the MVS services currently running on a specific host and port. You can also display the MVS status and the full list of pools.

In the left pane, click the **MVS Services** link to view the MVS services. The services are displayed in table format. Click the column name to sort the table by that column.



5.1.5.1 MVS Monitoring Window Elements

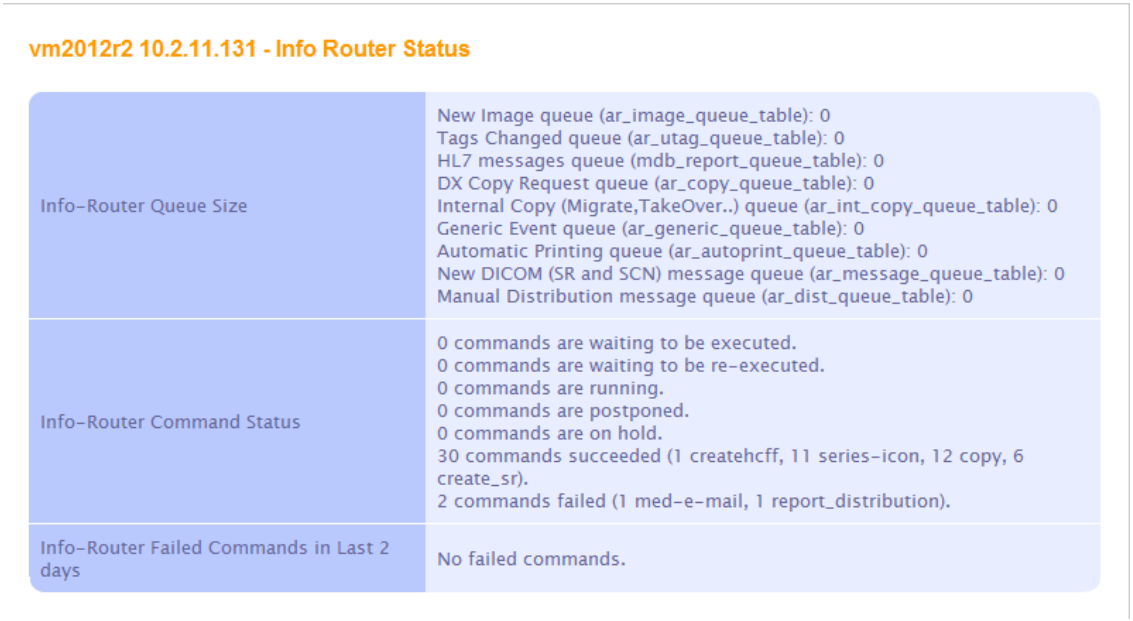
Element	Type	Description
Server List Window		
Port	List	Select the port type: non-secured or secured.
MVS Ping	Button	Click to display the MVS status on the specific host and port. The details shown include: • MVS version • Grid name • Node name • Issuer name.
Test Bandwidth	Button	See Section 5.1.7, Monitoring the Bandwidth.
Service List	Button	Click to display the MVS services currently running.
Pool List	Button	Click to display the list of pools that exist in MVS (even if no service of the pool is currently up). See Pool List Window.
Service Name	Column	The name of the MVS service.
Pool Name	Column	The name of the pool of the service.
PID	Column	The process ID number of the service.
Status	Column	The status of the service.
User	Column	The user associated with the service.
Request Duration	Column	The amount of time that the current request is being handled (for busy services only).

Element	Type	Description
# Requests	Column	The number of requests the service has handled since it started.
Pool Status	Hyperlink	Click to view details of the pool status and queue details in a new window.
Restart Pool	Hyperlink	Click to restart all service of the specific pool. The page refreshes immediately after the pool is restarted.
Analyze Pool	Hyperlink	Click to view statistics for the pool in a new window. Statistics shown include the requests rate and the busy services and pending requests.
Pool List Window		
#	Column	The row number.
Pool Name	Column	The name of the MVS pool.
Pool Status	Column	The pool status and the time the status was checked.
Pool Queue Details	Column	The pool status.
Pool Status	Hyperlink	Click to view details of the pool status and queue details in a new window.
Restart Pool	Hyperlink	Click to restart all services of the specific pool. The page refreshes immediately after the pool is restarted.
Analyze Pool	Hyperlink	Click to view statistics for the pool in a new window. Statistics shown include the requests rate and the busy services and pending requests.

5.1.6 Viewing the Info Router Status

You can view the Info Router status, including the Info Router queue size, command status, and failed commands.

In the left pane, click the **Info Router Status** link to view the Info Router status.



5.1.7 Monitoring the Bandwidth

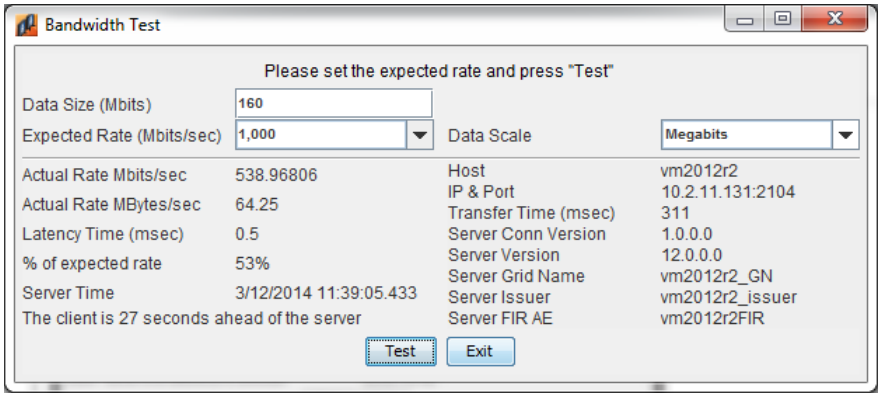
You can measure the bandwidth, or throughput of the network, by measuring the time required to transfer a file of known size using the conn protocol. You can do the following:

- Test the bandwidth between your workstation and the local node
- Test the bandwidth between the local node and remote nodes
- Test the bandwidth between server nodes using the command line

5.1.7.1 Testing the Bandwidth from Your Workstation

To test the bandwidth between your workstation and the local node:

1. To run a bandwidth test from the Administration Tool, select **System Monitor > Bandwidth Test** from the Administration Tool menu. The **Bandwidth Test** window opens.



2. In the **Bandwidth Test** window, you can change the data size, expected rate and data scale. Click **Test** to run the bandwidth test.

The bandwidth test results appear in the window.

3. Click **Exit** to close the window.

5.1.7.2 Testing the Bandwidth between Server Nodes

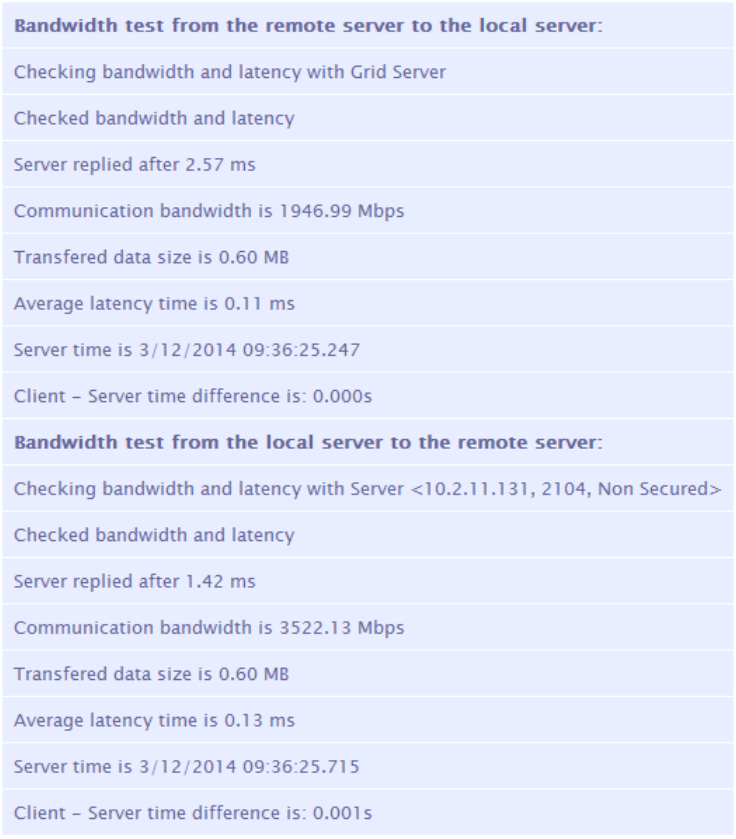
You can test the bandwidth between server nodes for the following PACS components:

- Vue PACS and external Vue Motion
- Vue PACS and Vue PACS
- Vue PACS and other grid nodes

The test is bidirectional, from the remote server to the local server and vice versa. The latency is tested three times.

To test the bandwidth between server nodes:

1. To run a bandwidth test from the System Monitoring & Control Tool, select **System Monitor > System Check** from the Administration Tool menu. The System Monitoring & Control tool opens showing menu links in the left pane.
2. In the left pane, click the **MVS Services** link.
3. Click the **Test Bandwidth** button. The bandwidth test results appear.



4. To change the expected bandwidth and size of data to transfer in the test, select the required value from the **Data Size (Megabits)** list.

5.1.7.3 Using the Command Line

You can measure the bandwidth between server nodes for PACS components by running bandwidth and latency tests, together or separately, from the command line. You can also run the command line utility from the Vue PACS client installation folder. Example commands include:

- For a remote server:
  tool_ping -i <server_name/ip> -p <port> -b <size> -lt <times>
- For a grid server:
  tool_ping -g <grid_name> -b <size> -lt <times>
- For a grid server using a secure connection:
  tool_ping -g <grid_name> -b <size> -lt <times> --secure

Command Line Parameters

`-g`	The grid name.
`-i`	The machine name or IP address. The default is `localhost`.
`-p`	The port number. The default is `2104`.
`-r`	The number of times to repeat the ping.
`-s`	The sleep time between repetitions, in milliseconds.
`-b`	The expected bandwidth and size of data to transfer in the test, in Mbps.
`-lt`	The number of consecutive latency tests to perform.
`-o`	Use to open a connection and hold it open.

`-t`	The timeout. The default is 10 seconds.
`--slow`	Force a slow connection.
`--secure`	Force a secure connection.
`--fast`	Force a fast connection.
`--nonsecure`	Force a nonsecure connection.
`-l`	Print the routing table.
`-h`	Help.

5.2 Using the Info Router

You can use the Info Router client to monitor rules that determine how images and other data are routed within the CARESTREAM PACS system and under what conditions the images are sent.

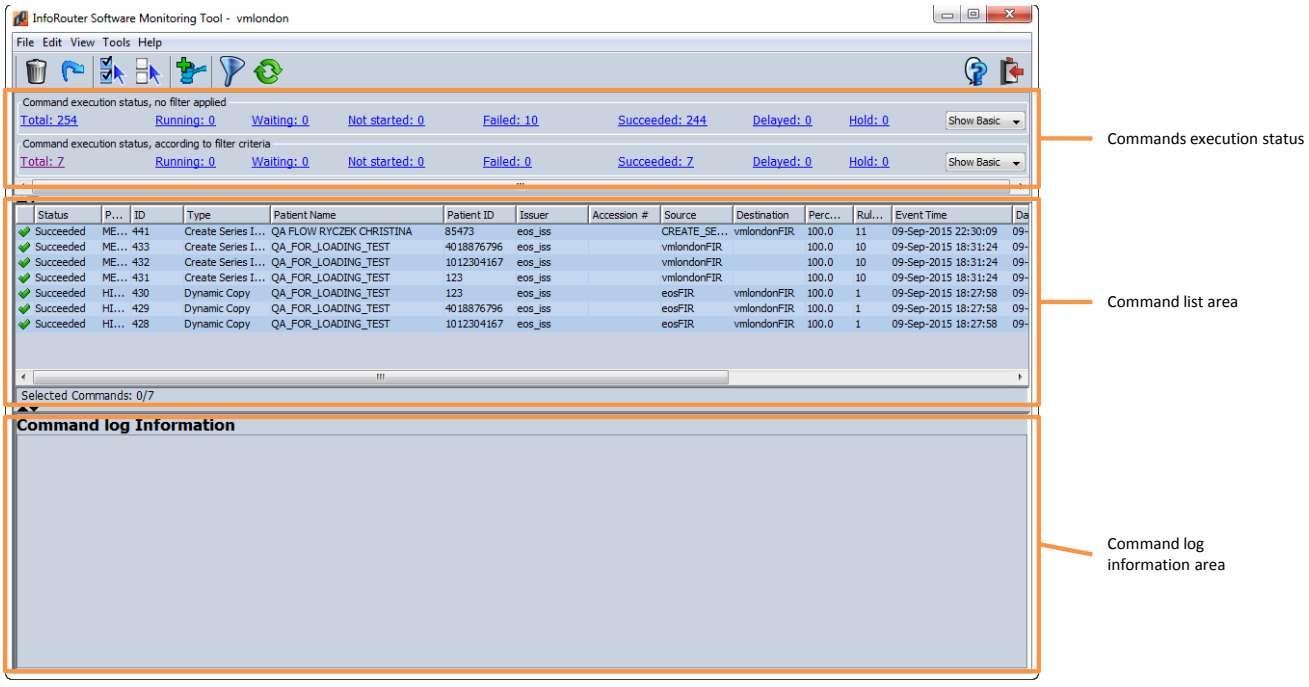
The Info Router client is accessible even in cases where Info Router server processes are down.

The Info Router client automatically synchronizes with the server, enabling you to create and update rules, as well as view existing rules and their related data. You can also create aliases for items and groups of items, and apply conditions to them.

5.2.1 Getting Started with the Info Router Client

To open the Info Router client, select **System Monitor > Info Router** from the Administration Tool menu.

The Info Router client opens showing the commands execution status, the command list area, and the command log information area.



The commands execution status panes display the status as shortcuts. To view information about each status, click the shortcut.

Screen splitter arrows between the areas enable you to resize the Command Log Information area, or click and drag it to a new position.

The number of commands displayed in the Info Router client can be controlled by applying filters.

5.2.1.1 Using the Info Router Client Toolbar

#	Description
1	**Delete the selected command(s)**— Click to delete the selected commands
2	**Retry the execution of the selected command(s)**— Click to retry the execution of the selected commands
3	**Select All**—Click to select all items
4	**Select None**—Click to remove selections
5	**Show Rules**—Click to show rules in the Rules window
6	**Filter**—Click to filter the results shown
7	**Refresh**—Click to refresh the display with the latest information
8	**Help**— Not in use
9	**Exit**—Click to close the application

5.2.1.2 Command List Area

The Command List area displays all commands created from all the active rules, together with general information and the current status of each command. For each command, it includes the following information:

- ID—The unique identification number for each command, according to the order in which the commands were created. When a command is deleted, the remaining commands retain their original identification numbers.
- Type—The type of command.
- Patient Name—The name of the patient.
- Source—The name of the source device from which the image or study is copied.
- Destination—The name of the destination device to which the image or study is being copied.
- Status—The current operational status of the command. Possible values are:
    - Running—The command is being executed. If the command previously failed, the number in brackets indicates the number of retries.
    - Waiting—The system is waiting for the next Running session, if the command previously failed.
    - Succeeded—The command was successfully executed.
    - Failed—The command failed.
- Date Started—The date and time when the command initially started to run.
- Date Completed—The date and time when the command succeeded or failed.

- Percent Completed—The percentage of completion of the command currently running. The display resets to 0% each time there is a retry.

5.2.1.3 Command Log Information Area

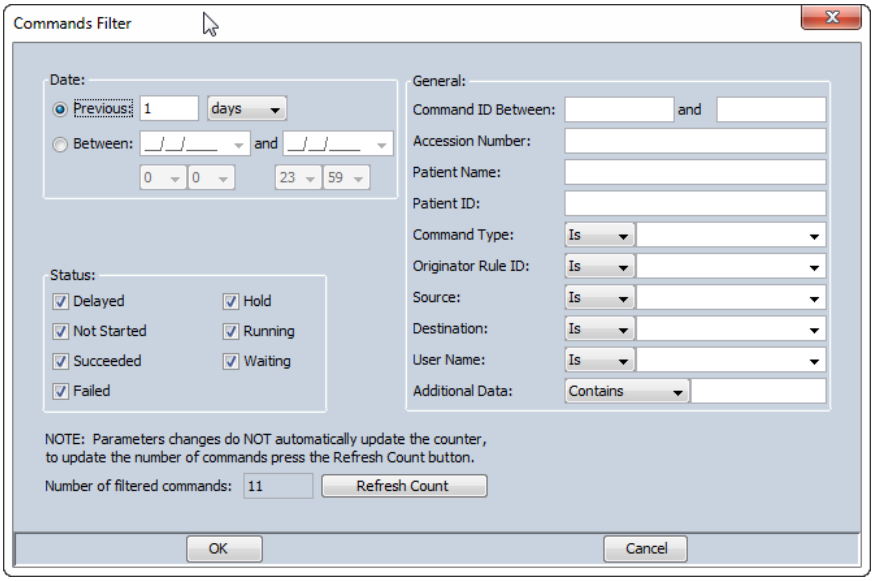
The Command Log Information area displays a running log of information for the command currently selected in the Command List area.

5.2.1.4 Filtering Commands

You can filter the commands that are displayed in the Command List area of the Monitor tab. You can also view the number of commands that appear in the Command List area when the filters are applied.

You should apply the appropriate command filters to reduce the number of commands that appear in the Command List area of the Monitor tab. When fewer commands appear, the retrieval time is reduced.

1. From the Info Router toolbar, click **Filter**  or from the **View** menu, select **Filter**. The **Commands Filter** window appears.



2. In the **Date** section, use the following options to filter commands by date:
   - **Previous**—Shows commands initiated in a predetermined number of days, hours, or minutes.
   - **Between Dates**—Shows commands initiated between the specified dates.
3. In the **Status** section, select the relevant status check boxes, such as **Not Started**, **Waiting**, and **Running**.
4. In the **General** section, complete the relevant parameters, as follows:
   - Command ID Between—The ID of the command from which to start the display. If you leave this field blank, all commands created up to the selected command in the **To ID** field are displayed.
   - Command Type—The type of command, such as **Dynamic Copy** or **Group SR**.
   - Originator Rule ID—The rule that generated the command.
   - Patient Name—The name of the patient. Enter a partial name to display all the patient names that begin with that string of letters.

- Source—The source of the event.
- Destination—The destination of the event.

5. The **Number of filtered commands** box displays the number of commands that are shown if filters are applied. To update the counter, click **Refresh Count**. The button is disabled if there are no changes.
6. Click **OK** to apply the selected filters.

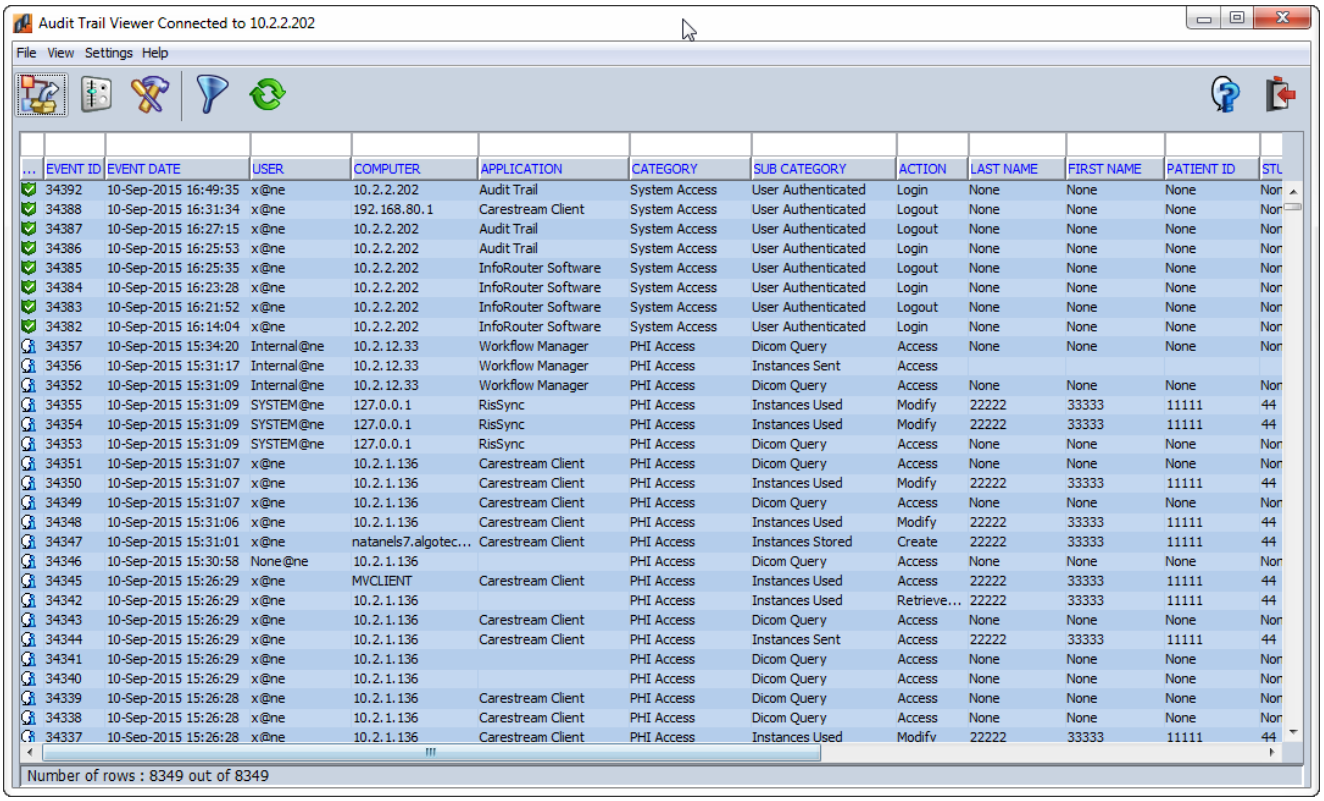
   The information in the Commands List area is updated and displayed according to the criteria you defined.

5.3 Using the Audit Trail Viewer

You can use the Audit Trail Viewer to track all PHI-related activities, warnings, and failures that occur in the system. You can then exclude events from auditing and define filters to manage information collected by the system. This information can be used to trace the source of selected changes to information in the system, as well as to detect unusual system activity.

5.3.1 Getting Started with the Audit Trail Viewer

1. To open the Audit Trail Viewer, select **System Monitor > Audit Trail** from the Administration Tool menu.
2. In the **Filter Events** window, enter any relevant parameters to filter the events shown. See Section 5.3.1.3 Filtering Events for more information.
3. Click **OK**. The **Audit Trail Viewer** window opens showing a list of events.



...	EVENT ID	EVENT DATE	USER	COMPUTER	APPLICATION	CATEGORY	SUB CATEGORY	ACTION	LAST NAME	FIRST NAME	PATIENT ID	STU
	34392	10-Sep-2015 16:49:35	x@ne	10.2.2.202	Audit Trail	System Access	User Authenticated	Login	None	None	None	Non
	34388	10-Sep-2015 16:31:34	x@ne	192.168.80.1	Carestream Client	System Access	User Authenticated	Logout	None	None	None	Non
	34387	10-Sep-2015 16:27:15	x@ne	10.2.2.202	Audit Trail	System Access	User Authenticated	Logout	None	None	None	Non
	34386	10-Sep-2015 16:25:53	x@ne	10.2.2.202	Audit Trail	System Access	User Authenticated	Login	None	None	None	Non
	34385	10-Sep-2015 16:25:35	x@ne	10.2.2.202	InfoRouter Software	System Access	User Authenticated	Logout	None	None	None	Non
	34384	10-Sep-2015 16:23:28	x@ne	10.2.2.202	InfoRouter Software	System Access	User Authenticated	Login	None	None	None	Non
	34383	10-Sep-2015 16:21:52	x@ne	10.2.2.202	InfoRouter Software	System Access	User Authenticated	Logout	None	None	None	Non
	34382	10-Sep-2015 16:14:04	x@ne	10.2.2.202	InfoRouter Software	System Access	User Authenticated	Login	None	None	None	Non
	34357	10-Sep-2015 15:34:20	Internal@ne	10.2.12.33	Workflow Manager	PHI Access	Dicom Query	Access	None	None	None	Non
	34356	10-Sep-2015 15:31:17	Internal@ne	10.2.12.33	Workflow Manager	PHI Access	Instances Sent	Access				
	34352	10-Sep-2015 15:31:09	Internal@ne	10.2.12.33	Workflow Manager	PHI Access	Dicom Query	Access	None	None	None	Non
	34355	10-Sep-2015 15:31:09	SYSTEM@ne	127.0.0.1	RisSync	PHI Access	Instances Used	Modify	22222	33333	11111	44
	34354	10-Sep-2015 15:31:09	SYSTEM@ne	127.0.0.1	RisSync	PHI Access	Instances Used	Modify	22222	33333	11111	44
	34353	10-Sep-2015 15:31:09	SYSTEM@ne	127.0.0.1	RisSync	PHI Access	Dicom Query	Access	None	None	None	Non
	34351	10-Sep-2015 15:31:07	x@ne	10.2.1.136	Carestream Client	PHI Access	Dicom Query	Access	None	None	None	Non
	34350	10-Sep-2015 15:31:07	x@ne	10.2.1.136	Carestream Client	PHI Access	Instances Used	Modify	22222	33333	11111	44
	34349	10-Sep-2015 15:31:07	x@ne	10.2.1.136	Carestream Client	PHI Access	Dicom Query	Access	None	None	None	Non
	34348	10-Sep-2015 15:31:06	x@ne	10.2.1.136	Carestream Client	PHI Access	Instances Used	Modify	22222	33333	11111	44
	34347	10-Sep-2015 15:31:01	x@ne	natanels7.algotec...	Carestream Client	PHI Access	Instances Stored	Create	22222	33333	11111	44
	34346	10-Sep-2015 15:30:58	None@ne	10.2.1.136		PHI Access	Dicom Query	Access	None	None	None	Non
	34345	10-Sep-2015 15:26:29	x@ne	MVCLIENT	Carestream Client	PHI Access	Instances Used	Access	22222	33333	11111	44
	34342	10-Sep-2015 15:26:29	x@ne	10.2.1.136		PHI Access	Instances Used	Retrieve...	22222	33333	11111	44
	34343	10-Sep-2015 15:26:29	x@ne	10.2.1.136	Carestream Client	PHI Access	Dicom Query	Access	None	None	None	Non
	34344	10-Sep-2015 15:26:29	x@ne	10.2.1.136	Carestream Client	PHI Access	Instances Sent	Access	22222	33333	11111	44
	34341	10-Sep-2015 15:26:29	x@ne	10.2.1.136		PHI Access	Dicom Query	Access	None	None	None	Non
	34340	10-Sep-2015 15:26:29	x@ne	10.2.1.136		PHI Access	Dicom Query	Access	None	None	None	Non
	34339	10-Sep-2015 15:26:28	x@ne	10.2.1.136	Carestream Client	PHI Access	Dicom Query	Access	None	None	None	Non
	34338	10-Sep-2015 15:26:28	x@ne	10.2.1.136	Carestream Client	PHI Access	Dicom Query	Access	None	None	None	Non
	34337	10-Sep-2015 15:26:28	x@ne	10.2.1.136	Carestream Client	PHI Access	Instances Used	Modify	22222	33333	11111	44

5.3.1.1 Using the Audit Trail Viewer Toolbar

#	Description
1	**Export logs in view to csv file**—Click to export the logs to a CSV file
2	**Display Settings**—Click to update the refresh interval
3	**Audit Settings**—Click to update general settings, such as the audit status and the maximum number of rows to fetch
4	**Filter**—Click to filter the results shown
5	**Refresh**—Click to refresh the display with the latest information
6	**Help**— Click to open the About window with copyright information
7	**Exit**—Click to close the application

5.3.1.2 Defining the Display in the Audit Trail Viewer

In the Audit Trail Viewer tool, a default set of fields is displayed. You can change the default view and choose which fields to display, the order in which they are displayed, and the width of each column.

You can make the following changes to the display:

To:	Do this:
Move a column	Left-click the column header and drag the column to the right or left.
Delete a column	Right-click the column to delete and select **Remove Column**.
Change the column width	Left-click the edge between two adjacent column headings and drag to the position you want.
Add a column	Right-click anywhere on the column header, select **Field Chooser**, and click **Add**.
Remove a column	Select a field in the right pane, select **Field Chooser**, and click **Remove**.
Save changes for future sessions	Right-click anywhere in the column header and select **Save Settings**.
Reset the filters	Right-click any column in the right pane and select Clear All Filters.
Reset the default settings	Right-click anywhere in the column header and select Set Default Settings.

5.3.1.3 Filtering Events

You can filter the events displayed in the **Audit Trail Viewer** window to display a manageable number of events and reduce consumption of system resources.

You can apply a single filter or use multiple filter criteria, as required. If filters have been applied, the filter criteria are displayed in the relevant filter fields (white fields above the column names).

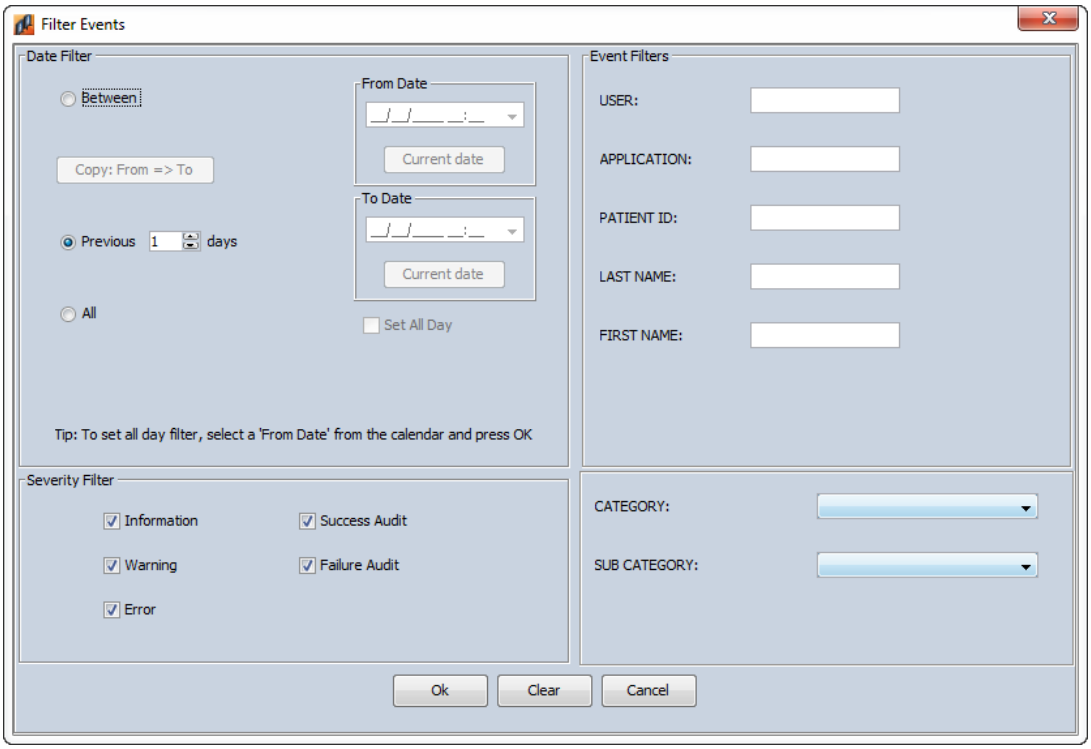
To apply a single filter to the events list:

1. In the events list area, click in the filter criteria field above the required column heading.
2. In the filter window that appears, enter the required filter criteria. To remove existing filter data, click **Clear**.
3. Click **OK**.

   The events list is filtered according to the filter you selected. The filter criteria appear in the field above the relevant column name.

To apply multiple filters to the events list:

1. From the Audit Trail Viewer toolbar, click **Filter**  or from the **View** menu, select **Filter Events**. The **Filter Events** window appears.



2. In the **Date Filter** section, use the following options to filter events by date:
   - **Between**—Shows events that occurred between the specified dates. Use DD/MM/YYYY format. To use the current date, click **Current date**.
   - **Previous**—Shows commands initiated in a predetermined number of days.

3. In the **Severity Filter** section, select the relevant event types to display, as follows:
    - Information—events related to PHI accesses, such as a data query or login.
    - Warning—events that could affect the system, such as major configuration changes or start/stop operations (for example, stopping the Info Router). Any changes made to the list of events that are not audited, are also considered warning events.
    - Error—events that indicate any type of failure that affects the availability of the system.
    - Success Audit—events such as successful logins to the system and other security-related matters.
    - Failure Audit—events that indicate a security violation, such as an authentication failure (bad login) or an access control restriction violation attempt.
4. In the **Event Filters** section, complete the relevant parameters, as follows:
    - User—the name of the user who performed the action recorded by the event.
    - Application—the source of the event, such as the Central Configuration.
    - Patient ID—the patient ID of the event:
    - Last Name—the patient's last name.
    - First Name—the patient's first name.

    Note: Partial entries and wildcards can be used in these fields.
5. Then select the following items:
    - Category—the event type, such as System Access or Account Management.
    - Sub Category—the event subtype, such as User Authentication or Security Alert.
6. Click **OK** to apply the selected filters. The list of events is updated automatically according to the filter criteria specified.

    OR

    Click **Clear** to clear existing filter criteria. You can then reset the filter criteria or click **OK** to close the window.

5.3.1.4 Sorting the Display

You can sort the information displayed in the Audit Trail Viewer window.

Click a column heading to sort the entire list by that item in ascending order. Click the same column heading again to sort the list in descending order.

You can sort the events displayed in the Audit Trail Viewer window using up to three columns.

1. Click once on a column heading to perform an ascending sort. Click the same column heading again to perform a descending sort.
2. Press Shift and click another column heading to select a secondary sort.
3. Press Ctrl and click another column heading to perform a tertiary sort.

If a column is used for a sort, a symbol is displayed next to the column name, as follows:

Symbol	Description
	First sort ascending
	Second sort ascending
	Third sort ascending
	First sort descending
	Second sort descending
	Third sort descending

5.3.1.5 Refreshing the Display

The Audit Viewer Tool window is updated with the latest information.

You can manually refresh the events displayed in the Audit Trail Viewer, as follows:

- From the Audit Trail Viewer toolbar, click **Refresh**  .
- From the **View** menu, select **Refresh**.

The currently displayed events are updated and displayed according to the latest information in the archive.

5.3.2 Archiving an Audit

You can use the Audit Trail Viewer to periodically export and archive data after a specific time.

IMPORTANT: It is the responsibility of the site to back up exported data.

For example, if the script runs once a month, the data from the previous month is exported and archived. An additional script allows the user to import the archived data back to the database so the user can view its contents.

5.3.3 Exporting Logs to MICROSOFT EXCEL

You can export logs in the Audit Trail Viewer and store them on your computer in a CSV (comma separated value) format.

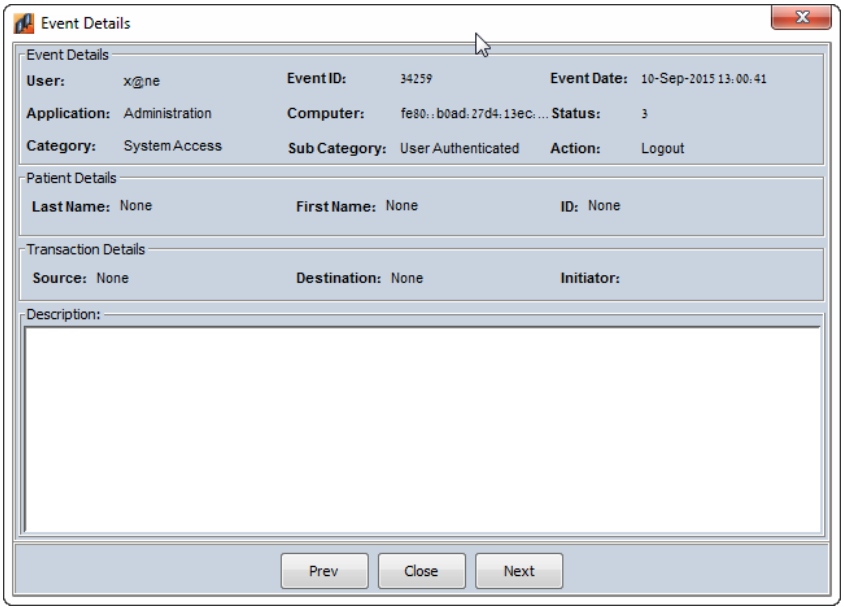
1. From the Audit Trail Viewer toolbar, click Export  .
2. In the **Export Audit to File** window, select the location to save the file.
3. Click **OK**.

5.3.4 Viewing Event Details

You can view the details of an event in a separate pop-up window, as required.

1. Select the required event in the events list.
2. From the **View** menu, select **Event Details** or double-click the required event.

   The **Event Details** window appears.



The **Event Details** window includes the most important information about the selected event, such as the event description, the category/subcategory, and the operation.

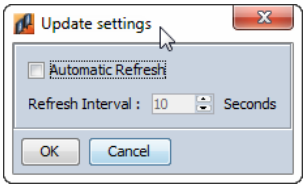
3. You can click the **Prev** and **Next** buttons to view the details of other events in the events list.

Note: The fields displayed in the **Event Details** window are fixed and do not reflect the selections made in the **Add/Remove Fields** window.

5.3.5 Defining Display Settings

You can define the automatic refresh interval for the events that display in the Audit Trail Viewer.

1. From the Audit Trail Viewer toolbar, click **Display Settings**  or from the **Settings** menu, select **Display Settings**. The **Update Settings** window appears.



2. To automatically update the events displayed in the Audit Trail Viewer, select the **Automatic Refresh** check box.
3. In the **Refresh Interval** field, enter a number or use the arrows to select refresh interval in seconds.
4. Click **OK** to save the settings.

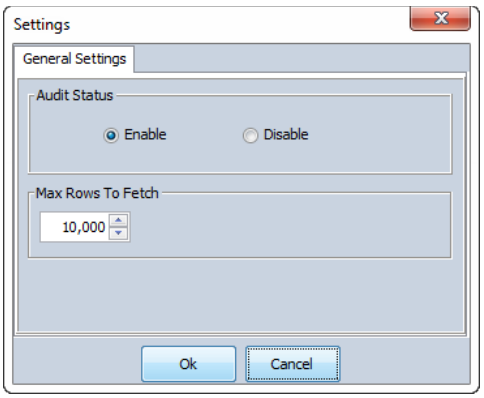
5.3.6 Defining Auditing Settings

You can enable or disable the auditing function. When the auditing function is disabled, no events that take place in the system are recorded.

Note: The auditing feature of the CARESTREAM PACS system is a critical last line of defense against misuse of the information contained in the system. It should never be disabled, except by authorized personnel in consultation with Carestream Health, Inc.

1. From the Audit Trail Viewer toolbar, click **Audit Settings**  or from the **Settings** menu, select **Audit Settings**.

   The **Settings** window appears.



2. To enable auditing, in the **Audit Status** section, select **Enable**.
3. In the Max Rows To Fetch section, enter a number or use the arrows to select the maximum number of rows to fetch.
4. Click **OK**.

Note: Enabling and disabling the auditing function are considered Warning-level events. If you choose to disable the auditing function, this operation is recorded as the last event before auditing stops.

5.3.7 Viewing History

The History Viewing function allows you to view audits either online or offline. Audits that are kept offline prevent the list of the Audit Trail Viewer from become overloaded. The time parameters for when events are taken offline is configurable.

From the **View** menu, choose **Select Audit Repository**.

Choose **Audit Offline**.

The offline Audit View trail appears.

5.4 Using the Synchronization Monitor

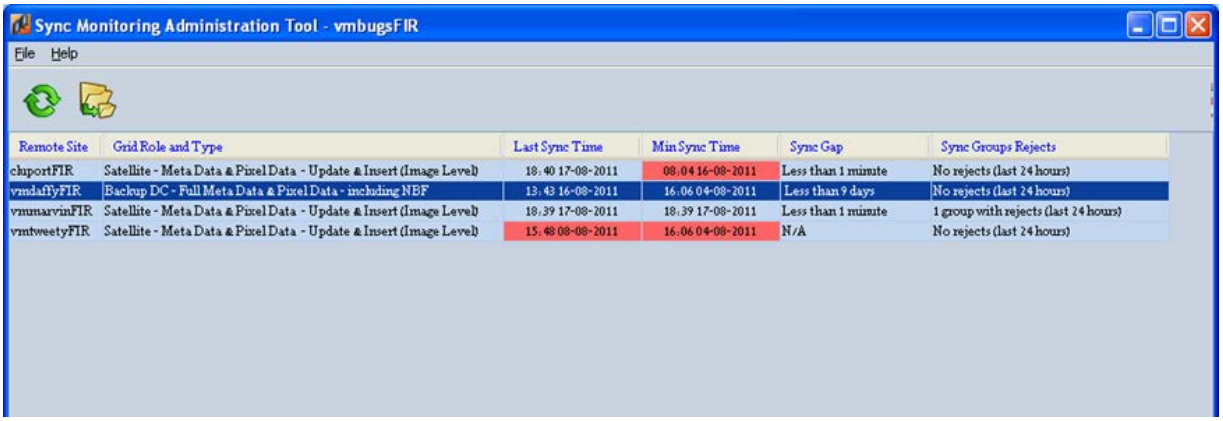
In grid and cluster environments, data is synchronized between the server nodes using the SMARTSYNCH tool. You can use the Synchronization Monitor to view the synchronization status and any synchronization errors, if they exist.

5.4.1 Getting Started with the Synchronization Monitor

You access the Synchronization Monitor from the target side, for example, from the data center or from the primary archive.

From the target server, select **System Monitor > Synchronization Monitor** from the Administration Tool menu.

The Synchronization Monitor opens showing the current status of each archive being synchronized. Fields with synchronization errors appear as red or yellow fields.

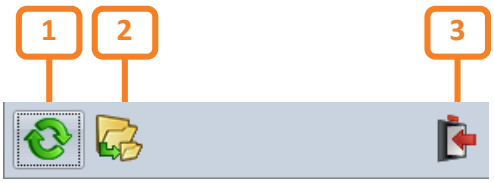


For each of the archives, you can view the following information:

Field	Description
Remote Site	The name of the remote site that is being synchronized. Archives that are configured but do not run are displayed as grayed out.
Grid Role and Type	The grid role and type of the archive. Examples of grid roles include archive data centers, satellites, and synchronized backup servers. Examples of types include metadata and pixel data, metadata only, and pixel data only.
Last Sync Time	The last time a successful synchronization was performed. This indicates whether the synchronization mechanism is working well with this archive. A failure here indicates that there is a general error, such as incorrect configuration, network failure, or some major application problem on the source or target archive (for example, `sync_main` or `sysync` are not running).
Min Sync Time	The minimum synchronization time. This indicates whether the synchronization mechanism is working well for all the operations and groups of this archive. A failure here indicates that there is an error for one or more groups, though others may be working properly. This may be due to an application error, a performance problem, or corrupted data.
Sync Gap	Indicates that the synchronization mechanism is working but is running behind.
Sync Groups Rejects	Displays the number of synchronization groups that have synchronization rejects for this archive in the last 24 hours.

Note: Disabled operations and groups are not included when calculating the values.

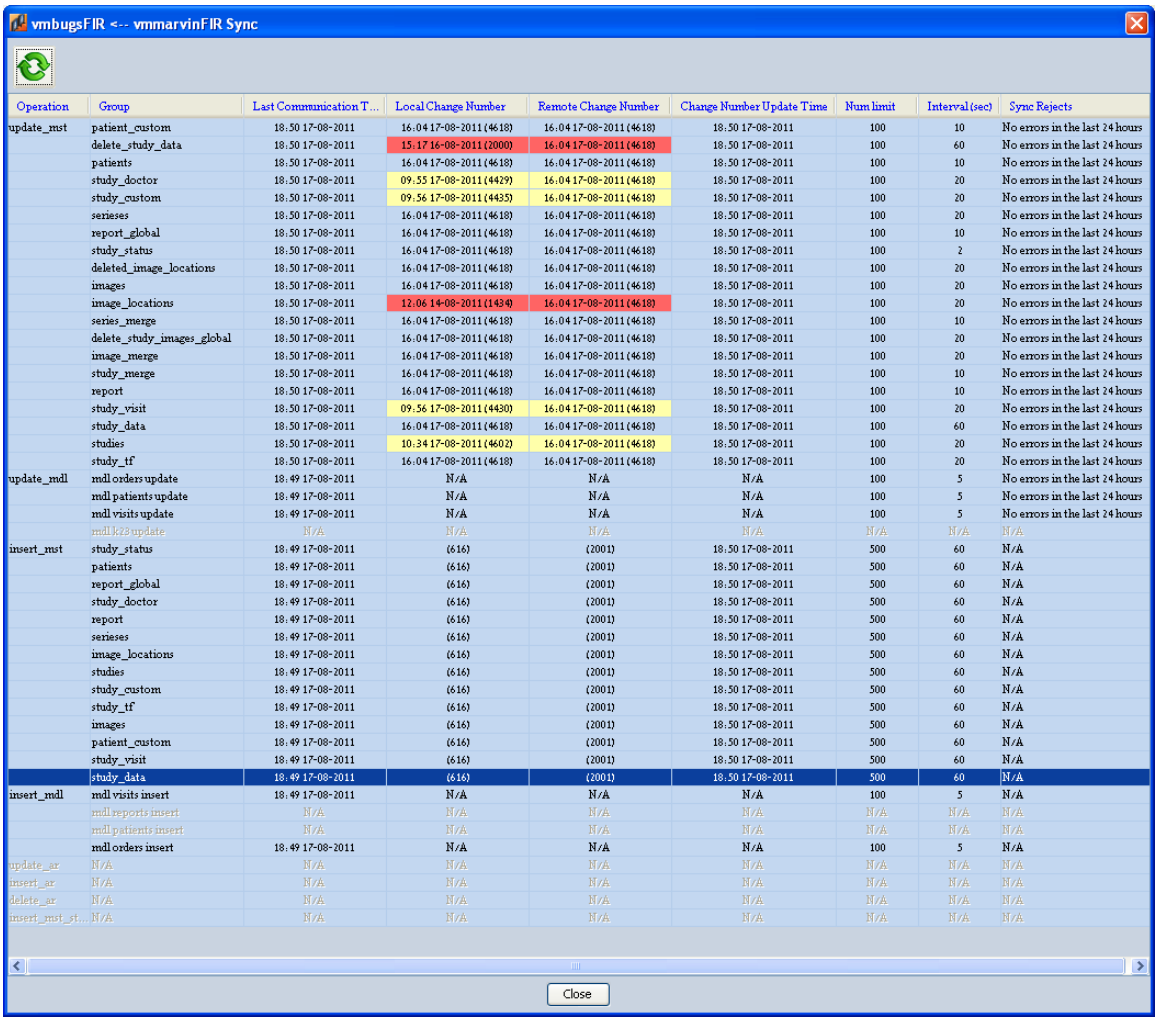
5.4.1.1 Using the Synchronization Monitor Toolbar



#	Description
1	**Refresh List**—Click to manually refresh the data that appears in the display area.
2	**Explore Node**—Click to view more details of synchronization operations and groups for an archive.
5	**Exit**—Click to close the application

5.4.2 Viewing Synchronization Details

In the Synchronization Monitor, double-click an archive to display more details of SMARTSYNC operations and groups for that archive.



Operation	Group	Last Communication T...	Local Change Number	Remote Change Number	Change Number Update Time	Num limit	Interval (sec)	Sync Rejects
update_mst	patient_custom	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	10	No errors in the last 24 hours
	delete_study_data	18:50 17-08-2011	15.17 16-08-2011 (2000)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	60	No errors in the last 24 hours
	patients	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	10	No errors in the last 24 hours
	study_doctor	18:50 17-08-2011	09.55 17-08-2011 (4429)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	study_custom	18:50 17-08-2011	09.56 17-08-2011 (4435)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	serieses	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	report_global	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	10	No errors in the last 24 hours
	study_status	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	2	No errors in the last 24 hours
	deleted_image_locations	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	images	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	image_locations	18:50 17-08-2011	12.06 14-08-2011 (1434)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	series_merge	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	10	No errors in the last 24 hours
	delete_study_images_global	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	image_merge	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	study_merge	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	10	No errors in the last 24 hours
	report	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	10	No errors in the last 24 hours
	study_visit	18:50 17-08-2011	09.56 17-08-2011 (4430)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	study_data	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	60	No errors in the last 24 hours
	studies	18:50 17-08-2011	10.34 17-08-2011 (4602)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
	study_tf	18:50 17-08-2011	16.04 17-08-2011 (4618)	16.04 17-08-2011 (4618)	18:50 17-08-2011	100	20	No errors in the last 24 hours
update_mdl	mdl orders update	18:49 17-08-2011	N/A	N/A	N/A	100	5	No errors in the last 24 hours
	mdl patients update	18:49 17-08-2011	N/A	N/A	N/A	100	5	No errors in the last 24 hours
	mdl visits update	18:49 17-08-2011	N/A	N/A	N/A	100	5	No errors in the last 24 hours
	mdl k23 update	N/A	N/A	N/A	N/A	N/A	N/A	N/A
insert_mst	study_status	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	patients	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	report_global	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	study_doctor	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	report	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	serieses	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	image_locations	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	studies	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	study_custom	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	study_tf	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	images	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	patient_custom	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	study_visit	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
	study_data	18:49 17-08-2011	(616)	(2001)	18:50 17-08-2011	500	60	N/A
insert_mdl	mdl visits insert	18:49 17-08-2011	N/A	N/A	N/A	100	5	N/A
	mdl reports insert	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	mdl patients insert	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	mdl orders insert	18:49 17-08-2011	N/A	N/A	N/A	100	5	N/A
update_ar	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
insert_ar	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
delete_ar	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
insert_mst_st...	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

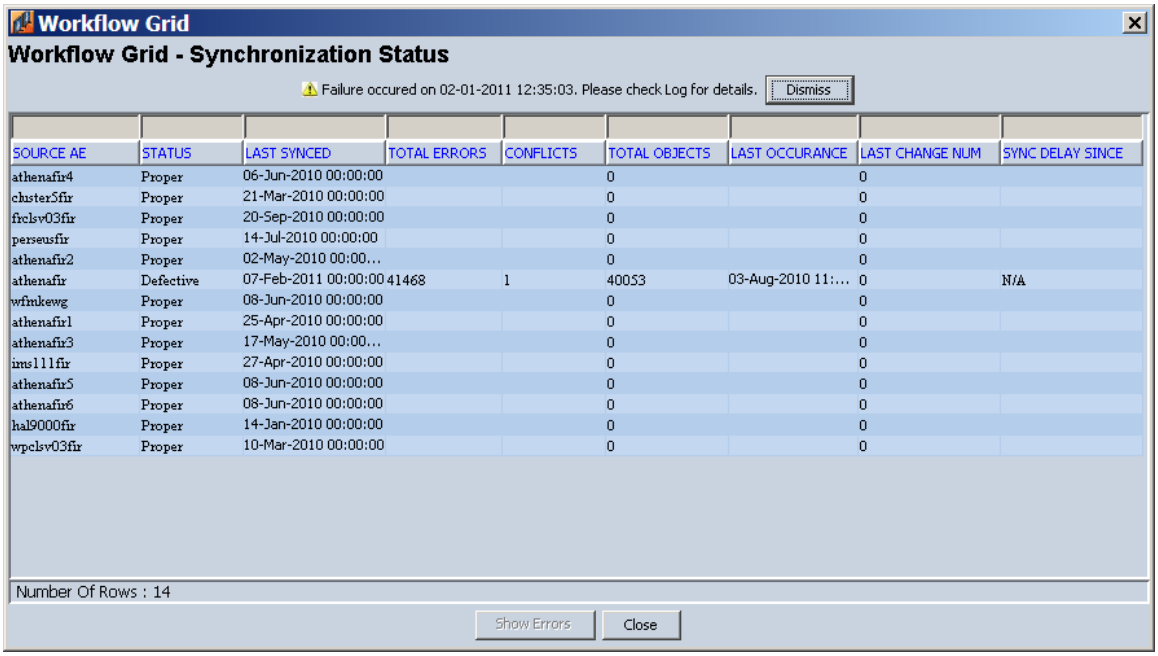
For the selected archive, you can view the following information:

Field	Description
Operation	The operation that is being synchronized. Operations that are configured but do not run are displayed as grayed out.
Group	The group that is being synchronized. Groups that are configured but do not run are displayed as grayed out.
Last Communication Time	The last time a successful synchronization was performed for this group.
Local Change Number Remote Change Number	The local change number indicates the last synchronized change. The remote change number indicates the latest change waiting to be synchronized. These values are compared to get the Sync Gap, which indicates whether the synchronization mechanism is working but is running behind.
Change Number Update Time	The time when the displayed data in the Local Change Number and Remote Change Number columns was modified. Notice that the displayed data in the monitor is not modified on every change but on every interval.
Num Limit Interval (sec)	These configuration values provide a complete view of how often each group is synchronized and how many records are sent on each iteration. Combining these values with the Last Communication Time and Sync Gap helps to track down problems.
Sync Rejects	The number of synchronization errors for this group and archive in the last 24 hours.

5.4.3 Viewing Synchronization Errors in the Workflow Manager Administration Tool

You can also view synchronization errors from the Workflow Manager Administration tool.

1. Select **System Administration > Database Admin** from the Administration Tool menu.
2. From the **View** menu, select **Synchronization Errors**. The Workflow Grid window appears displaying any synchronization errors that have occurred.



From here, you can manually retry SMARTSYNC operations.

5.5 Comparing Archives

You can compare the contents of two archives to locate missing studies and identify mismatched data.

The archive compare mechanism compares the metadata of studies according to the following criteria:

- Range of study dates
- Filter on every DICOM tag supported by the system (such as the accession number and site ID)

It can be run on either the source archive or the target archive and applies to the following scenarios:

- Grid environment—compares metadata between the data center and a satellite
- Cluster environment—compares metadata between the primary archive and the backup server
- Archive replacement—compares two archives following a takeover process

The comparison can be run between two Workflow Manager archives, a Workflow Manager archive and a third-party DICOM archive, or between two third-party archives.

The archive compare mechanism issues a report with a list of missing studies, as well as studies with mismatched metadata. The report can be viewed and filtered in the Archive Compare tool.

5.5.1 Running the Archive Comparison

You can run the archive comparison using one of the following scripts:

- `archives_compare_safety.pl`—compares only patient-safety-related entities, such as the PID, patient name, birth date, and accession number.
- `archives_compare_dicom.pl`—compares all study-related entities.
- `archives_compare_hl7.pl`—compares all HL7 objects, including patients, orders and reports.

It is recommended that you create a daily scheduled task to run the archive comparison. You can also run it manually from the command line, if required.

Use the following syntax to run an archive comparison for a range of study dates:

```
/c Perl -IC:\PROGRA~1\Carestream\System5\scripts
C:\PROGRA~1\Carestream\System5\scripts\archives_compare_safety.pl -s <PrimaryFIR>
-t <StandbyFIR> -i <MIN_STUDY_DATE> -a <MAX_STUDY_DATE> >
C:\Users\CSHSER~1\AppData\Local\Temp\log_archive_compare_<sitename>.txt 2>&1
```

Default parameters for the archive comparison are configured in the Central Configuration Editor in the following location:

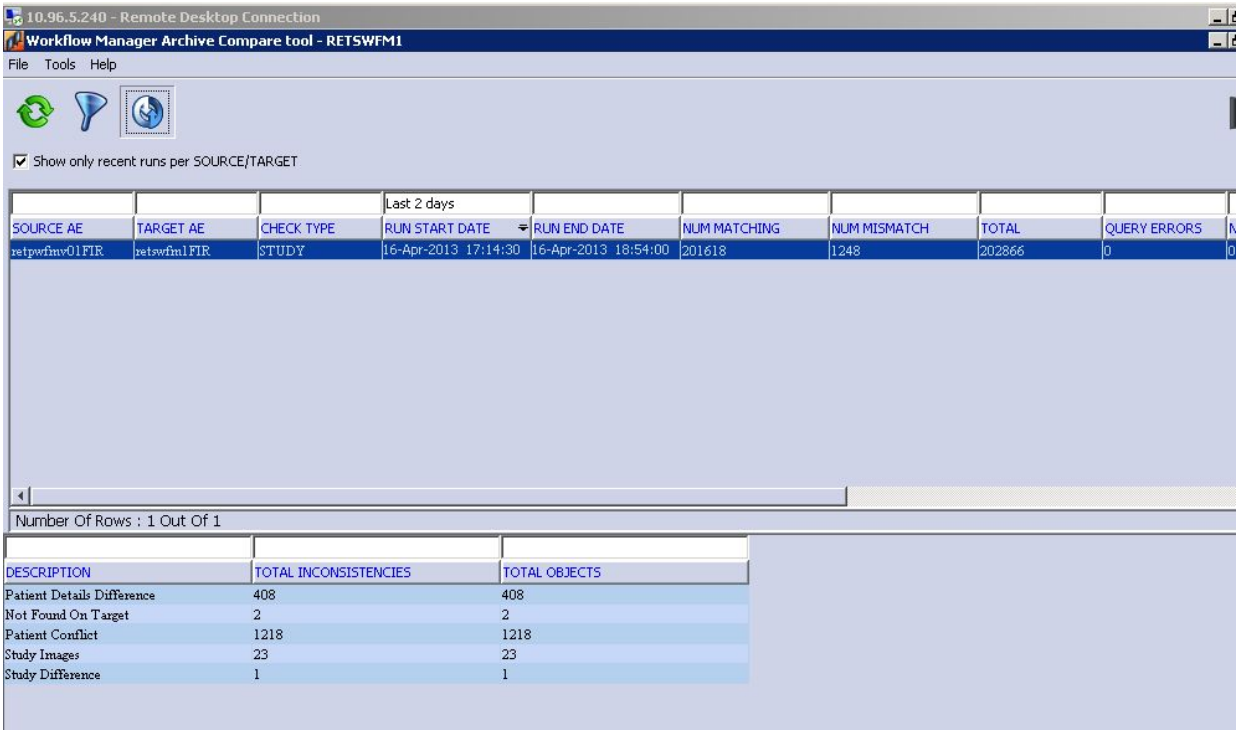
```
imaginet\system\applications\medistore\sync_check
```

5.5.2 Viewing the Results

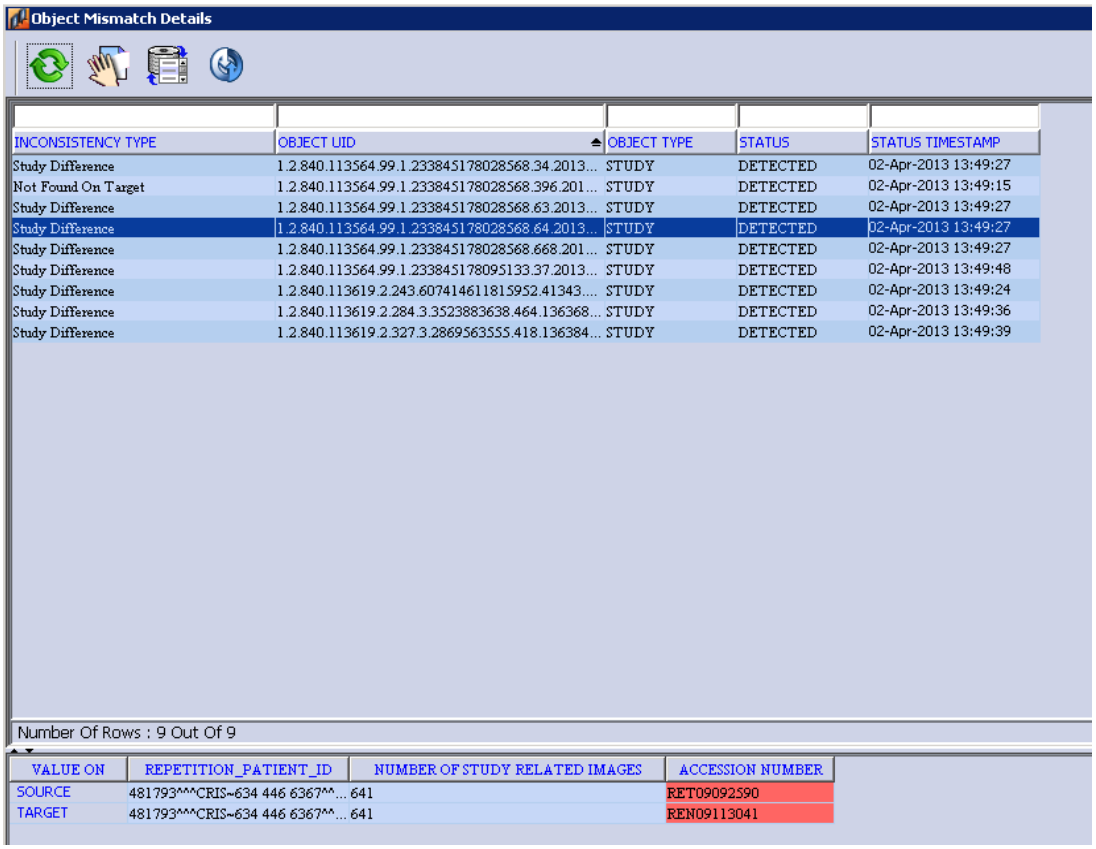
You can use the Archive Compare tool to view and filter the results of the archive comparison.

1. To open the Archive Compare tool, select **System Monitor > Archive Compare Tool** from the Administration Tool menu.
2. In the **Enter Filter Values** window, enter any relevant parameters to filter the archive comparison runs shown and click **OK**.

   The Archive Compare tool opens showing a list of recent archive comparisons.



3. Select a specific run to view the results summary in the bottom pane.
4. Double-click a specific run to view inconsistencies in the Object Mismatch Details window.



Select a specific inconsistency in the top pane to view in more detail in the bottom pane. The inconsistencies are highlighted in red.

5.5.2.1 Using the Archive Compare Toolbar

#	Description
1	**Refresh List**—Click to manually refresh the data that appears in the display area.
2	**Edit Filter**—Click to filter columns in the Object Mismatch Details window. (This button only appears in the Object Mismatch Details window.)
3	**View Filter Window**—Click to filter the data that appears in the display area.
4	**Run Fix**—Click to automatically fix mismatched data. If this fix is not successful, you must fix manually.
5	**Exit**—Click to close the application

5.5.2.2 Defining the Display in the Archive Compare Tool

In the Archive Compare tool, a default set of fields is displayed. You can change the default view and choose which fields to display, the order in which they are displayed, and the width of each column.

You can make the following changes to the display:

To:	Do this:
Move a column	Left-click the column header and drag the column to the right or left.
Delete a column	Right-click the column to delete and select **Remove Column**.
Change the column width	Left-click the edge between two adjacent column headings and drag to the position you want.
Add a column	Right-click anywhere on the column header, select **Field Chooser**, and click **Add**.
Remove a column	Select a field in the right pane, select **Field Chooser**, and click **Remove**.
Save changes for future sessions	Right-click anywhere in the column header and select **Save Settings**.
Reset the filters	Right-click any column in the right pane and select Clear All Filters.
Reset the default settings	Right-click anywhere in the column header and select Set Default Settings.

5.5.2.3 Filtering the Archive Comparison Results

You can apply the following types of filters to the archive comparison results:

- Source AE and Target AE Filter—Filters according to the source and target AEs.
- Start Run Date— Filters according to the start run date. There are two ways to enter this type of filter:
  - Between—Filters the studies list by the defined date range. Enter the **to** and **from** dates in DD/MM/YYYY format, or click Current Date to insert the current date for the relevant field.
  - Previous—Select or enter the number of previous days (for example, 7 for the previous week). All studies added to the archive during the previous [x] days appear.

You can apply a single filter or both filter criteria, as required. If filters have been applied, the filter criteria are displayed in the relevant filter fields (white fields above the column names).

Note: The **Enter Filter Values** window appears automatically when you open the Archive Compare tool. This lets you filter the runs included in the archive comparison results before the list is loaded, reducing the download time required to display the list.

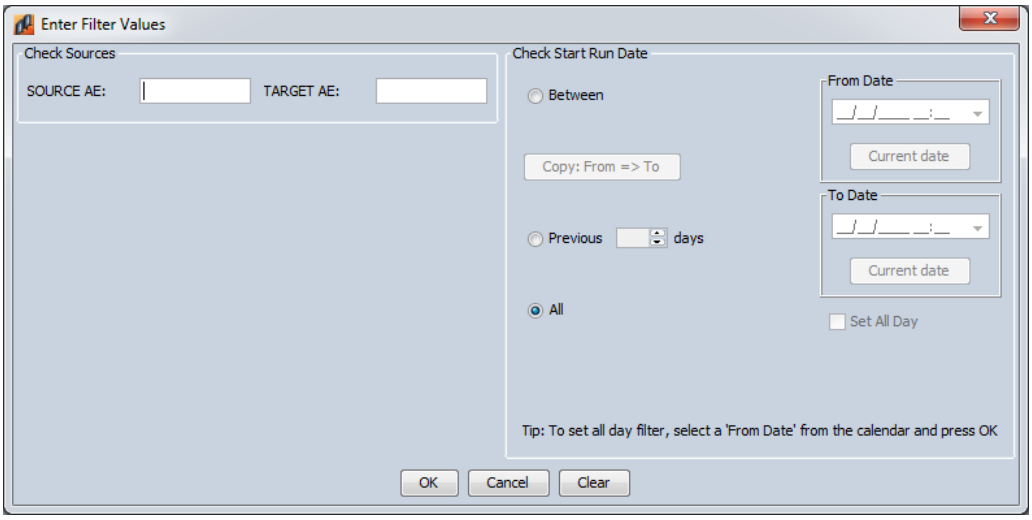
To apply a single filter to the archive comparison results list:

1. In the archive comparison results list area, click in the filter criteria field above the required column heading.
2. In the filter window that appears, enter the required filter criteria. To remove existing filter data, click **Clear**.
3. Click **OK**.

   The archive comparison results list is filtered according to the filter you selected. The filter criteria appear in the field above the relevant column name.

To apply both filters to the archive comparison results list:

1. From the Archive Compare toolbar, click **Filter**  or from the **Tools** menu, select **Filter Dialog**. The **Enter Filter Values** window appears.



2. Enter the required values in any combination of fields. To remove existing filter data, click **Clear**.
3. Click **OK**.

The archive comparison results list is filtered according to the filter criteria that you selected. The filter criteria appear in the fields above the relevant column names.

6 Performing Database Configuration and Management

This section describes the following tasks:

- Backing up the Database
- Restoring the Database
- Verifying the Database Backup
- Changing the Scheduled Time for the Database Backup
- Backing up the Central Configuration
- Checking the ORACLE Alert File
- Performing an ORACLE Server General Fitness Check
- Running Other Scheduled Database Maintenance Tasks

6.1 Backing up the Database

A daily backup of the entire database is performed using a MICROSOFT WINDOWS scheduled task, usually at night.

The backup method can be a hot backup, where the database is online and users can continue to work, or a cold backup, where the database is shut down and users are unable to work until the backup is complete. The backup method is chosen during installation.

The following scheduled tasks are defined:

- `run_full_backups` – Use to run hot backups
- `run_al_backups` – Use to run archive logs only backups
- `run_cold_backups` – Use to run cold backups

In a cluster configuration, these tasks are executed on the database node.

The backup process writes database backup files and log files to a location on a local disk that is chosen during installation, for example, `<Backup_drive>:\oradata\mst1\backup`.

Backup log files use the following naming convention:

`back_<type>.<status>_date.log`

Where:

`type` = `inc0` for a hot backup

`al` for an archive logs only backup

`cold` for a cold backup

`status` = `ok` or `err` indicating the success or failure of the backup process.

If backup storage allows, a backup should be kept for both the current backup and the previous backup.

The previous backup is saved in `<Backup_drive>:\oradata\mst1\backup\COPY`.

IMPORTANT: Backup files must be copied to a tape, network location, or other media, on a daily basis. Failure to do so might lead to a total site loss.

6.2 Restoring the Database

Full or partial restoration of a database from a backup should only be done by Customer Service. Any attempt by unqualified personnel may result in permanent loss of patient data or a general system malfunction.

The hot backup method uses the ORACLE RMAN utility and requires DBA skills for recovery. The cold backup method involves OS copy commands and does not require DBA skills for recovery.

6.3 Verifying the Database Backup

A daily task runs at 6 am to ensure that the previous backup was successful. You can also perform this backup verification manually when there is a related problem reported by the system check, as follows:

1. In WINDOWS, select Start > Control Panel > System and Maintenance > Administrative Tools > Task Scheduler.
2. Right-click **Open**.
3. Select the relevant scheduled task and check that the date in the **Last Run Time** column is today's date. The following scheduled tasks are defined:
    - `run_full_backups`
    - `run_al_backups`
    - `run_cold_backups`
4. Navigate to `<Backup_drive>:\oradata\mst1\backup` and check whether the name of the log file includes the status `ok` or `err`.

    If the name of the log file includes `err`, an error exists and you should contact Customer Service.

6.4 Changing the Scheduled Time for the Database Backup

You can change the scheduled time for the database backup, as follows:

1. In WINDOWS, select Start > Control Panel > System and Maintenance > Administrative Tools > Task Scheduler.
2. Right-click the relevant scheduled task and select **Properties**. The following scheduled tasks are defined:
    - `run_full_backups`
    - `run_al_backups`
    - `run_cold_backups`
3. In the **Schedule** tab, change the time as required and click **OK**.

6.5 Backing up the Central Configuration

Daily backups of the Central Configuration are performed each night using the following scheduled tasks:

- `run_cfg_backups` – Exports the configuration database schema to an ORACLE export file.
- `db_cfg_export` – Exports the XML configuration to a GZIP compressed file.

Export files are written to `<Backup_drive>:\Backup\cfg_backup.`

The backup files can be used to restore the system configuration to an earlier state without restoring the entire database (which is more complicated and takes longer).

History is kept for 7 days.

This task is executed on the database node in cluster configurations.

6.6 Checking the ORACLE Alert File

The ORACLE database has a built-in alert file, in which system alerts and important messages are registered. You should read this file daily to identify potential problems at an early stage, as follows:

1. Navigate to

   `<DB_drive>:\imaginet_db\oracle\admin\diag\rdbms\mst1\mst1\trace\alert_mst1.log`

   and open the alert file using Notepad or WordPad.
2. Scroll down to the last section of the file.
3. Locate the last week's dates and review the messages.

   Only informative messages are acceptable, such as startup, shutdown, and changing log files. (Thread 1 advanced to log sequence)

   If an error exists, contact Customer Service.

6.7 Performing an ORACLE Server General Fitness Check

When the system is restarted, or after a failure or invoked operation, such as installation, upgrade or restructuring, you must ensure that all of system components are functioning properly. You should perform the ORACLE Server general fitness check manually after every reboot.

When the system is up, these services should be running:

- `OracleServicemst1` – The Workflow Manager database service
- `OracleOraDB12Home1TNSListener` – The ORACLE Listener service

6.8 Running Other Scheduled Database Maintenance Tasks

The following table lists other daily tasks that are scheduled for database maintenance purposes.

Task Name	Description	Notes
DB_Tablespace_freespace	A daily task that handles ORACLE database tablespace management. This script enlarges relevant tablespaces by either enlarging current database files or adding new files.	This task is executed on the database node in cluster configurations.
db_worker	A daily task that collects database statistics of relevant tables and indexes. Database objects statistics are gathered to allow ORACLE to access data in the most efficient way.	This task is executed on the application node in cluster configurations.
OracleLogsHandler	A daily task that handles database log files, including ORACLE alert log files, and ORACLE listener log files and trace files. History is kept for 60 days.	This task is executed on the database node in cluster configurations.

Task Name	Description	Notes
gather_db_info	A daily task that collects database performance statistics for the last 24 hours. Information collected includes AWR reports, ORACLE configuration files, ORACLE logs, ORACLE database settings and host server information. History is kept for 60 days.	This task is executed on the database node in cluster configurations.

7 Performing System Administration Tasks

You can use System Administration tools to perform system administration tasks, including:

- Working with the Workflow Manager Administration Tool
- Working with IS Link
- Working with the Certificate Portal
- Working with the Central Configuration Editor

7.1 Working with the Workflow Manager Administration Tool

You can use the Workflow Manager Administration tool to view patient and study data, update and edit information, and perform more advanced manipulations, such as merging or splitting studies.

You can use the Workflow Manager Administration tool for the following activities:

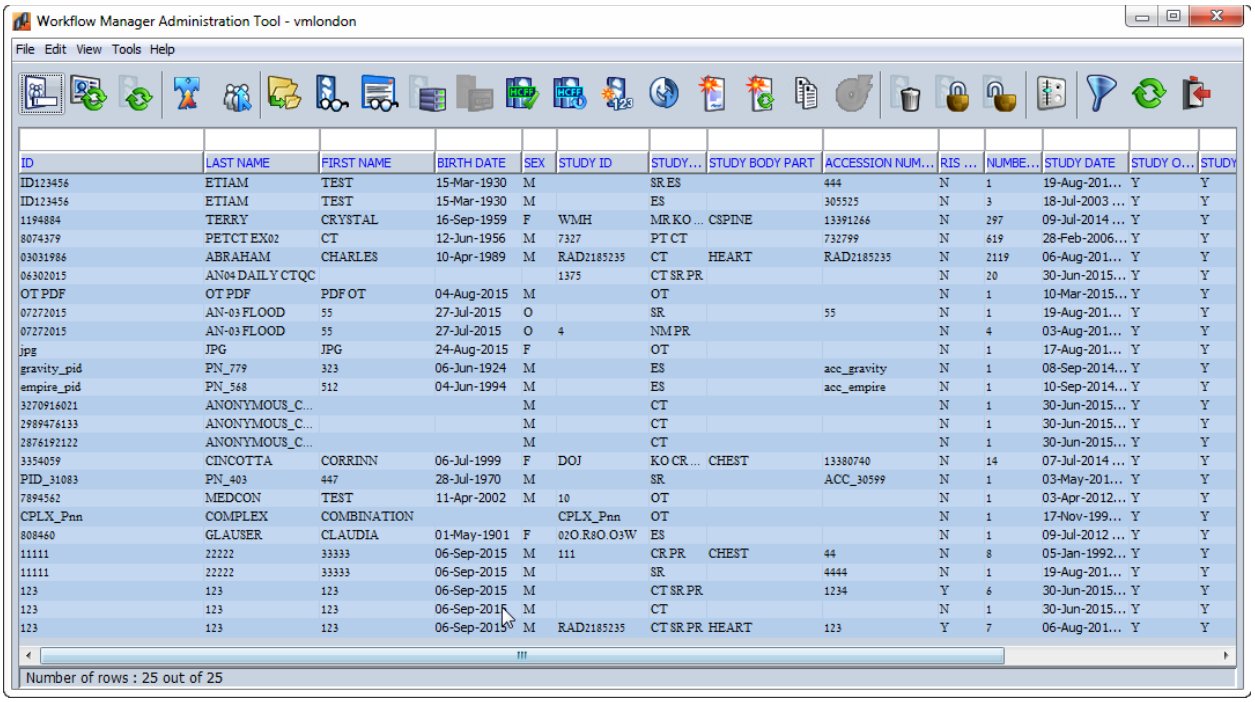
- Managing Patient IDs
- Updating Patient Details
- Updating Study Details
- Performing Merge and Split
- Updating Series Information
- Viewing Study Information
- Locating Studies
- Viewing Backup Media for Studies
- Performing Manual RIS Synchronization
- Protecting and Unprotecting Studies

7.1.1 Getting Started with the Workflow Manager Administration Tool

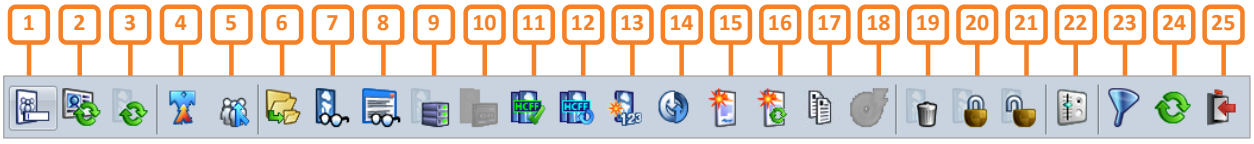
To open the Workflow Manager Administration tool, select **System Administration > Database Admin** from the Administration Tool menu.

In the **Enter Filter Values** window, enter any relevant parameters to filter the studies shown and click **OK**.

The Workflow Manager Administration tool opens showing a list of patient and study data.



7.1.1.1 Using the Workflow Manager Administration Toolbar



#	Description
1	**Manage Patient ID—**Click to open the **Manage Patient ID** window in which you can view, add or update a patient ID.
2	**Update Patient Details—**Click to update patient details for one or more patients.
3	**Update Study Details—**Click to update study details for one or more patients.
4	**Merge-Split Wizard**—Click to open the Merge Split wizard in which you can move studies from one patient to another.
5	**Merge Patients—**Click to move one or more studies from one patient to another.
6	**Explore Study—**Click to open the Series Details window for the study in which you can view more information about the series.
7	**View Study—**Click to view images for a selected study and any report information, if available.
8	**View Order—**Click to view the related order.
9	**Study Location—**Click to view the locations of one or more studies.
10	**Study Media—**Click to view the location of the backup media for one or more studies.
11	**Study Check HCFF—**Click to check the status of HCFF for a study.
12	**Study Rebuild HCFF—**Click to rebuild the HCFF of a study.

#	Description
13	**Change Study Instance UID**—Relevant for QCQ.
14	**Manual RIS-Synch—**Click to perform manual RIS synchronization on one or more studies.
15	**Create Structured Report—**Click to create a structured report for a study.
16	**Manual Distribution—**Click to manually re-distribute a report.
17	**DICOM Copy Study—**Click to manually DICOM copy a study.
18	**Burn Study—**Click to burn a study to a CD.
19	**Delete Study—**Click to delete a study.
20	**Protect Study—**Click to protect a study from deletion or changes.
21	**Unprotect Study—**Click to remove the protect status.
22	**Display Settings—**Click to configure the automatic refresh settings and the maximum number of rows that are displayed in the Studies List area.
23	**View Filter Window—**Click to filter the data that appears in the Studies List area.
24	**Refresh On-Line Studies—**Click to manually refresh the data that appears in the Studies List area.
25	**Exit**—Click to close the application.

The Workflow Manager Administration toolbar is page-sensitive; when toolbar functions are not relevant to a particular page, they are grayed out.

7.1.1.2 Defining the Display in the Workflow Manager Administration Tool

In the Workflow Manager Administration tool, a default set of fields at the study, series, and image level are displayed. You can change the default view and choose which fields to display, the order in which they are displayed, and the width of each column.

You can make the following changes to the display:

To:	Do this:
Move a column	Left-click the column header and drag the column to the right or left.
Delete a column	Right-click the column to delete and select **Remove Column**.
Change the column width	Left-click the edge between two adjacent column headings and drag to the position you want.
Add a column	Right-click anywhere on the column header, select **Field Chooser**, and click **Add**.
Remove a column	Select a field in the right pane, select **Field Chooser**, and click **Remove**.
Save changes for future sessions	Right-click anywhere in the column header and select **Save Settings**.
Reset the filters	Right-click any column in the right pane and select Clear All Filters.

To:	Do this:
Reset the default settings	Right-click anywhere in the column header and select Set Default Settings.

7.1.1.3 Filtering the Studies List

You can apply the following types of filters to the studies list:

- String Filter—Applies to columns that display data in string format and can accept any kind of string. Each string in the column that begins with the entered filter string passes through the filter and appears in the studies list.
- Date Filter— Applies to columns that display data in date format. There are two ways to enter this type of filter:
  - Between—Filters the studies list by the defined date range. Enter the **to** and **from** dates in DD/MM/YYYY format, or click Current Date to insert the current date for the relevant field.
  - Previous—Select or enter the number of previous days (for example, 7 for the previous week). All studies added to the archive during the previous [x] days appear.
- Numeric Filter—Applies to columns that display numbers. You can use a single number or a numeric range to filter columns.

You can apply a single filter or use multiple filter criteria, as required. If filters have been applied, the filter criteria are displayed in the relevant filter fields (white fields above the column names).

Note: The **Enter Filter Values** window appears automatically when you open the Workflow Manager Administration tool. This lets you filter the studies included in the studies list before the list is loaded, reducing the download time required to display the list.

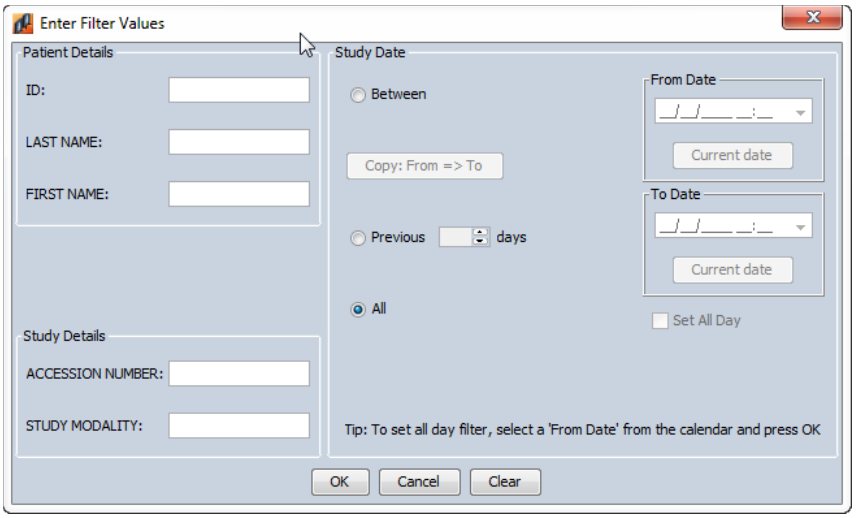
To apply a single filter to the studies list:

1. In the studies list area, click in the filter criteria field above the required column heading.
2. In the filter window that appears, enter the required filter criteria. To remove existing filter data, click **Clear**.
3. Click **OK**.

   The studies list is filtered according to the filter you selected. The filter criteria appear in the field above the relevant column name.

To apply multiple filters to the studies list:

1. From the Workflow Manager Administration toolbar, click **Filter**  or from the **View** menu, select **Filter Dialog**. The **Enter Filter Values** window appears.



2. Enter the required values in any combination of fields. To remove existing filter data, click **Clear**.
3. Click **OK**.

   The studies list is filtered according to the multiple filter criteria that you selected. The filter criteria appear in the fields above the relevant column names.

7.1.1.4 Sorting the Studies List

You can sort the studies list using up to three columns.

1. Click once on a column heading to perform an ascending sort. Click the same column heading again to perform a descending sort.
2. Press Shift and click another column heading to select a secondary sort.
3. Press Ctrl and click another column heading to perform a tertiary sort.

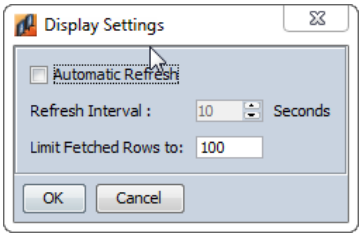
If a column is used for a sort, a symbol is displayed next to the column name, as follows:

Symbol	Description
	First sort ascending
	Second sort ascending
	Third sort ascending
	First sort descending
	Second sort descending
	Third sort descending

7.1.1.5 Configuring Display Settings

You can configure the interval at which the data displayed in the Workflow Manager Administration tool is automatically refreshed, as well as the maximum number of rows of data that are displayed.

1. From the Workflow Manager Administration toolbar, click **Display Settings**  or from the **Edit** menu, select **Display Settings**. The **Display Settings** window appears.



2. To activate the automatic refresh feature, select the **Automatic Refresh** check box.
3. In the **Refresh Interval** field, enter a number or use the arrows to select refresh interval in seconds.
4. In the **Limit Fetched Rows to** field, enter the maximum number of rows to appear in the studies list.

   Note: You can enter a value of 0 to display all studies, but the list may be so large that it is unworkable.

5. Click **OK**.

7.1.1.6 Refreshing the Studies List

You can manually refresh the list of studies displayed in the Workflow Manager Administration tool, as follows:

- From the Workflow Manager Administration toolbar, click **Refresh**  .
- From the **File** menu, select **Refresh**.
- Right-click a study from the studies list and select **Refresh**.

The currently displayed studies in the studies list are updated and displayed according to the latest information in the archive.

7.1.2 Managing Patient IDs

In the Workflow Manager Administration tool, the patient ID that is connected to the default issuer is shown in the study list. However, a single patient might have several different patient IDs provided by different issuers.

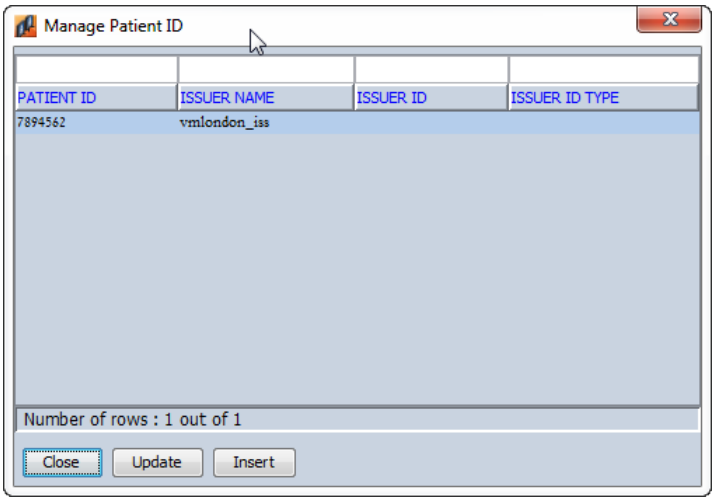
You can view, add, or update a patient ID. You can also delete a patient ID, however, this option is disabled by default. To change the default setting, go to:

```
imaginet\system\applications\medistore\admintool
```

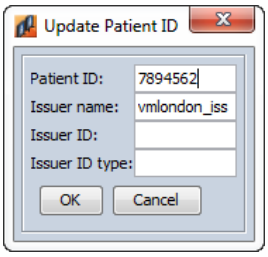
and set `allow_pid_delete` to `TRUE`.

To view, add, or update a patient ID:

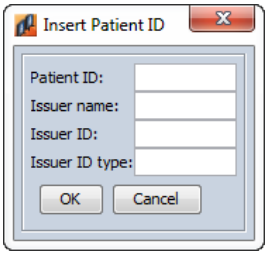
1. From the Workflow Manager Administration toolbar, click **Manage Patient ID**  . The **Manage Patient ID** window appears.



2. To update a patient ID, select the relevant row and click **Update**. In the **Update Patient ID** window, complete the changes as required and click **OK**.



3. To insert a new patient ID, click **Insert**. In the **Insert Patient ID** window, complete the changes as required and click **OK**.



4. Click **Close**.

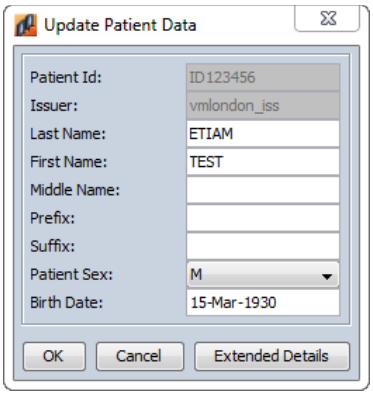
7.1.3 Updating Patient Details

You can update patient details, such as the patient's name, sex or birth date for an individual patient or for multiple patients at the same time.

1. Select the required study or studies in the studies list area.
2. Do one of the following:

   - From the Workflow Manager Administration toolbar, click **Update Patient Details** 
   - From the **Edit** menu, select **Update Patient**
   - Right-click the required study and select **Update Patient**

   The **Update Patient Data** window appears.



Note: If more than one study was selected, the **Patient ID** field is disabled and cannot be updated.

3. Update the patient data, as required.
4. Click **Extended Details** to update the phonetic or ideographic patient name details.
5. Click **OK**.

   The relevant patient data is updated in the archive.

Note: When patient data is modified, the change is applied to all the studies for this patient

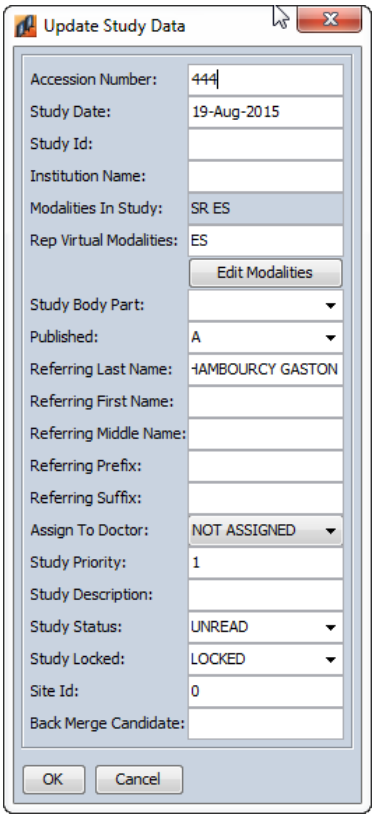
7.1.4 Updating Study Details

You can update study details, such as the study date, modality, body part, or study status for an individual patient or for multiple patients at the same time.

1. Select the required study or studies in the studies list area.
2. Do one of the following:

   - From the Workflow Manager Administration toolbar, click **Update Study Details** 
   - From the **Edit** menu, select **Update Study**
   - Right-click the required study and select **Update Study**

   The **Update Study Data** window appears.



3. To edit the modality of the study, click **Edit Modalities**.
4. In the **Update Series Modalities** window, select the relevant modality and click **OK**.
5. Update the study data, as required and click **OK**.

   The relevant study data is updated in the archive.

7.1.5 Performing Merge and Split Operations

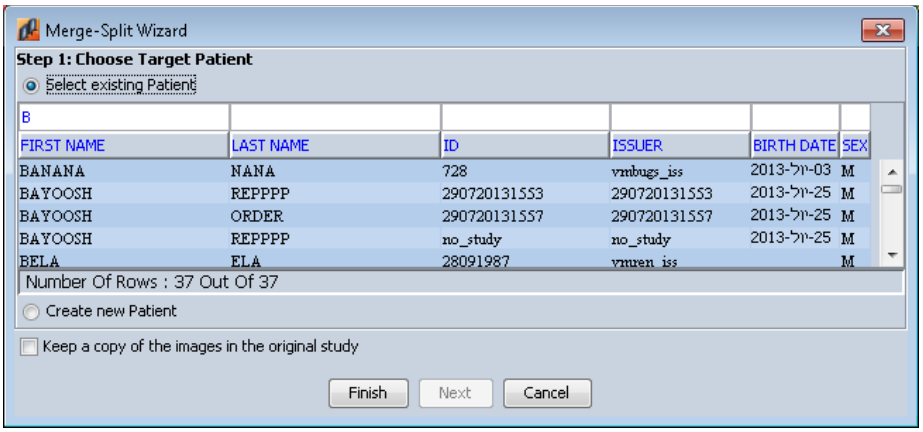
You can use the Merge-Split wizard to perform merge and split operations on studies and series.

The Merge operation is generally performed when a study is inserted and attached to an incorrect patient. The Merge operation lets you remedy this problem by moving the incorrectly attached study to the correct patient. You can move an individual study or multiple studies at the same time (for example, merge two studies with a third study).

7.1.5.1 Merging Studies

1. Select the relevant study or studies in the studies list area and click **Merge-Split Wizard**  .

   The **Merge-Split Wizard** window appears open on **Step 1: Choose Target Patient**.



2. Select the **Select existing Patient** option.
3. Filter the patient list, as required. Then select the required patient and click **Finish**.

   The incorrectly attached study merges with the selected patient information in the archive.

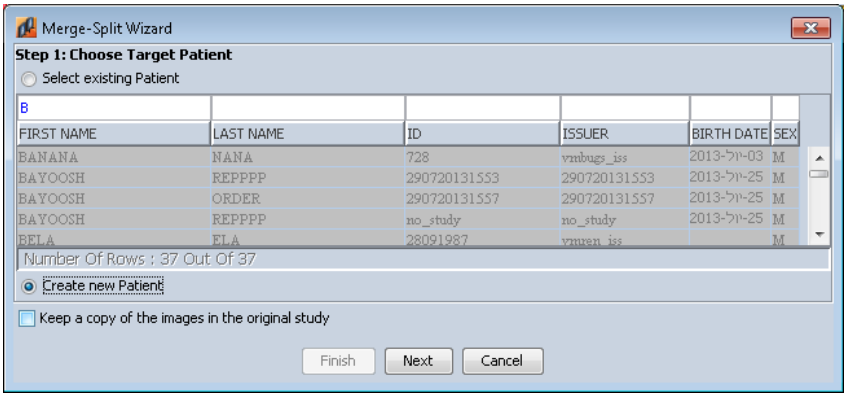
   Note: The Merge operation may take longer if you are merging multiple studies. In this case, an additional confirmation message appears, informing you that it will take some time and asking if you want to continue with the Merge operation.

7.1.5.2 Splitting Studies

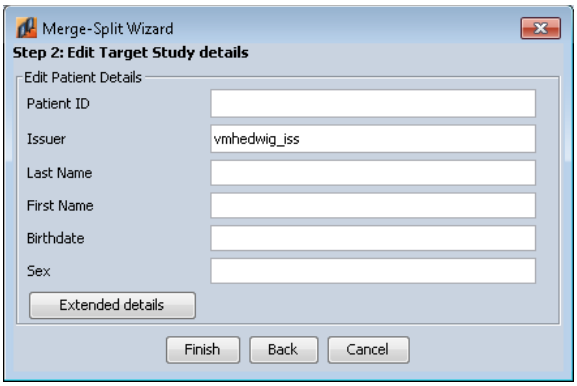
Sometimes modalities generate a single study, which contains multiple body parts (Chest/Abd/Pelvis) although there are separate orders for each body part. These studies can be split into multiple studies—one for each order.

1. Select the relevant study or studies in the studies list area and click **Merge-Split Wizard**  .

   The **Merge-Split Wizard** window appears open on **Step 1: Choose Target Patient**.



2. Select the **Create new Patient** option and click **Next**.
3. In the **Step 2: Edit Target Study Details** window, complete the new patient data, as required and click **Finish**.



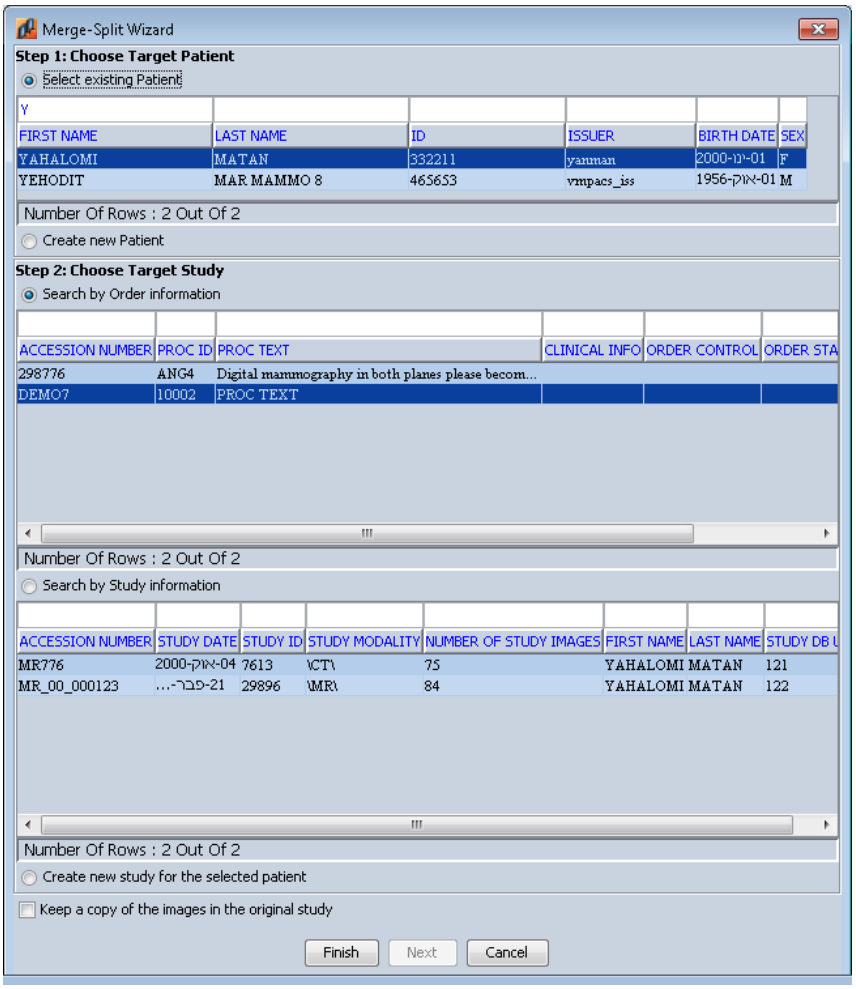
4. The study is attached to the newly-created patient information in the archive.

Note: The Split operation may require a longer time to perform if you are splitting multiple studies or if the selected study is comprised of numerous images.

7.1.5.3 Merging a Series from One Study to Another

1. In the **Series Details** window, select the series to merge and click **Merge-Split Wizard**  .

   The **Merge-Split Wizard** window appears.



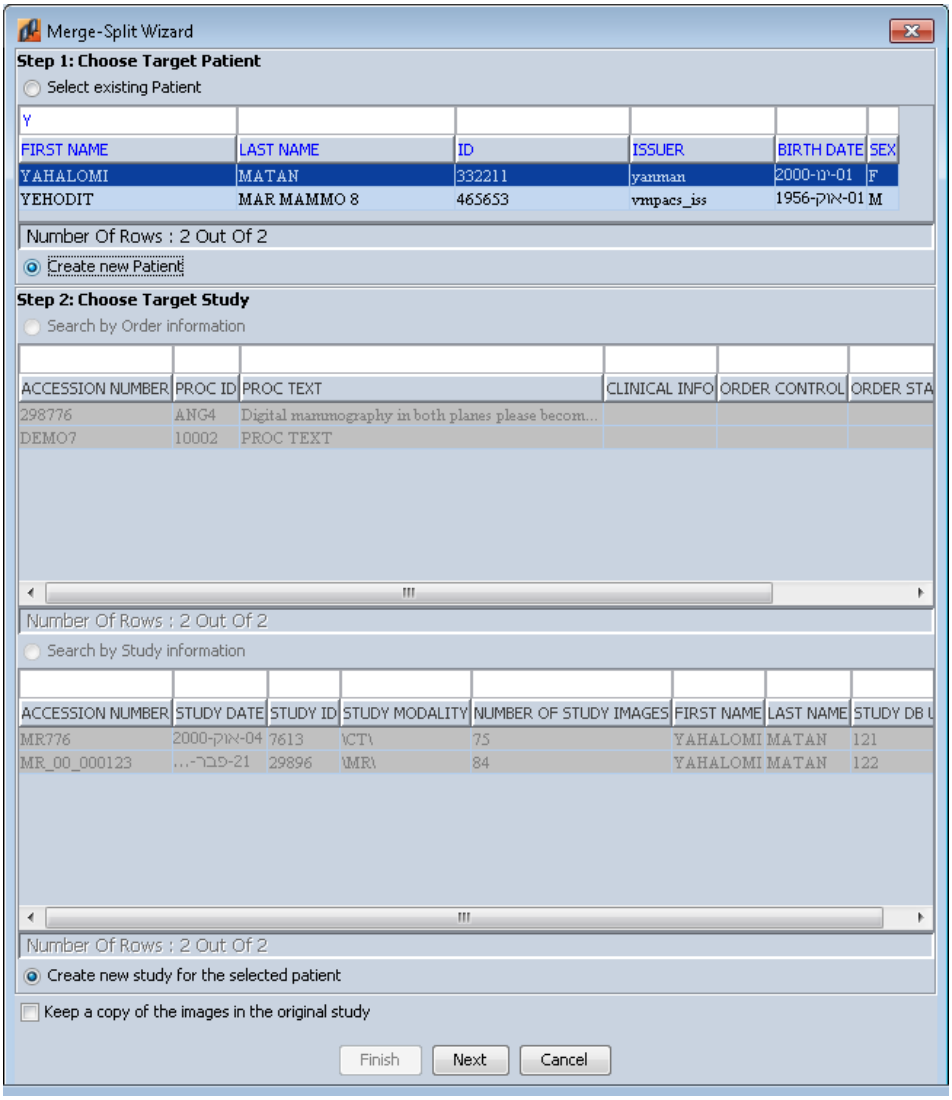
2. In the **Step 1: Choose Target Patient** section, select the **Select existing Patient** option.
3. Filter the patient list, as required. Then select the required patient.
4. In the **Step 2: Choose Target Study** section, select the relevant order or study. Then click **Finish**.

   The series is merged with the selected patient information in the archive.

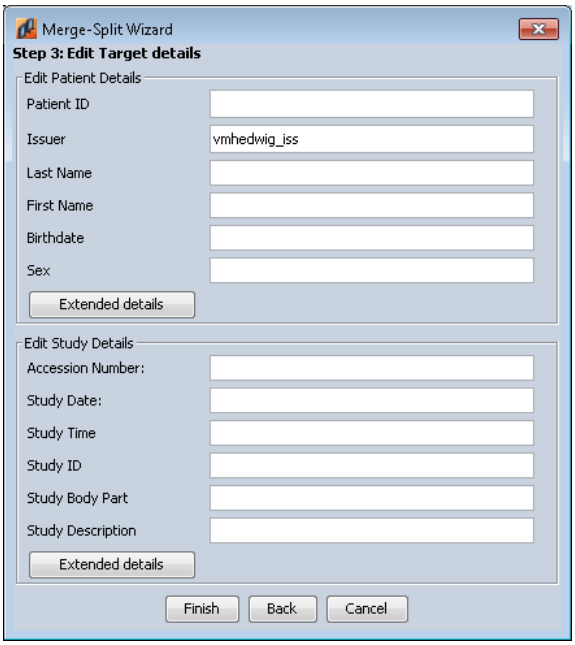
7.1.5.4 Splitting a Series

1. In the **Series Details** window, select the series to split and click **Merge-Split Wizard**  .

   The **Merge-Split Wizard** window appears.



2. Select the **Create new Patient** option and click **Next**.
3. In the **Step 2: Edit Target Study Details** window, complete the new patient data or study, as required and click **Finish**.



4. The study is attached to the newly-created patient information or study in the archive.

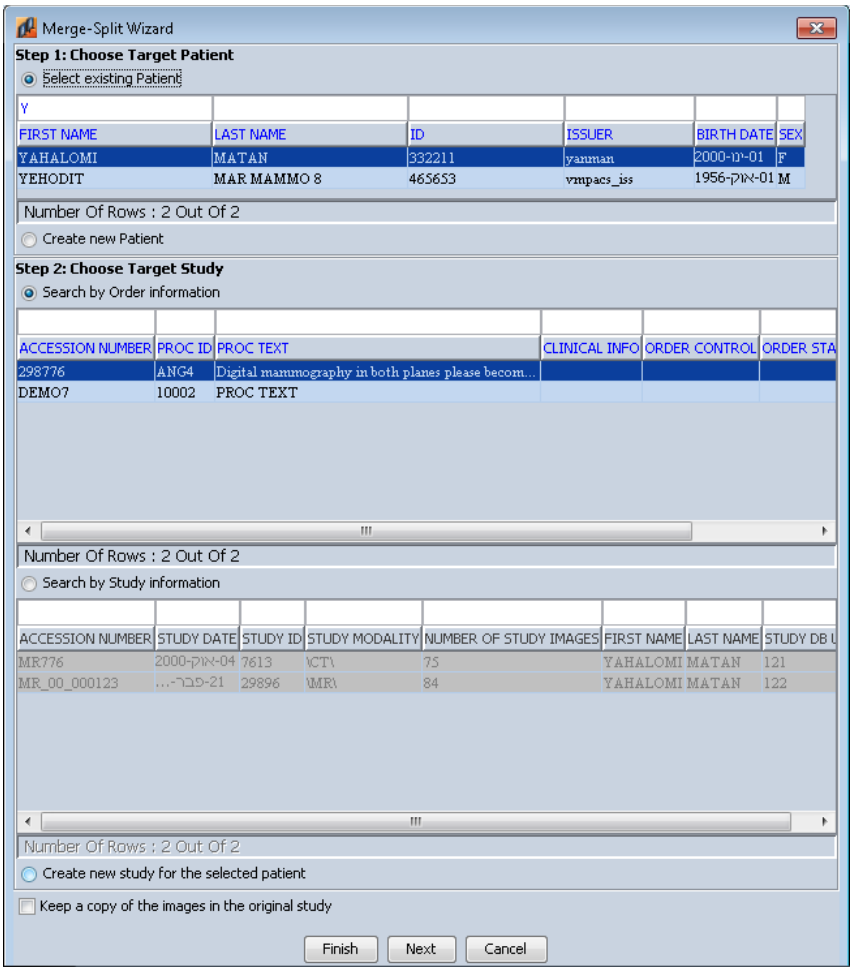
Note: The Split operation may require a longer time to perform if you are splitting multiple studies or if the selected study is comprised of numerous images.

7.1.5.5 Merging Images

You can merge an image to an existing patient, study, or series.

1. In the **Image Details** window, select the images to merge and click **Merge-Split Wizard**  .

   The **Merge-Split Wizard** window appears open on **Step 1: Choose Target Patient**.



2. Select the **Select existing Patient** option.
3. Filter the patient list, as required. Then select the required patient and click **Finish**.

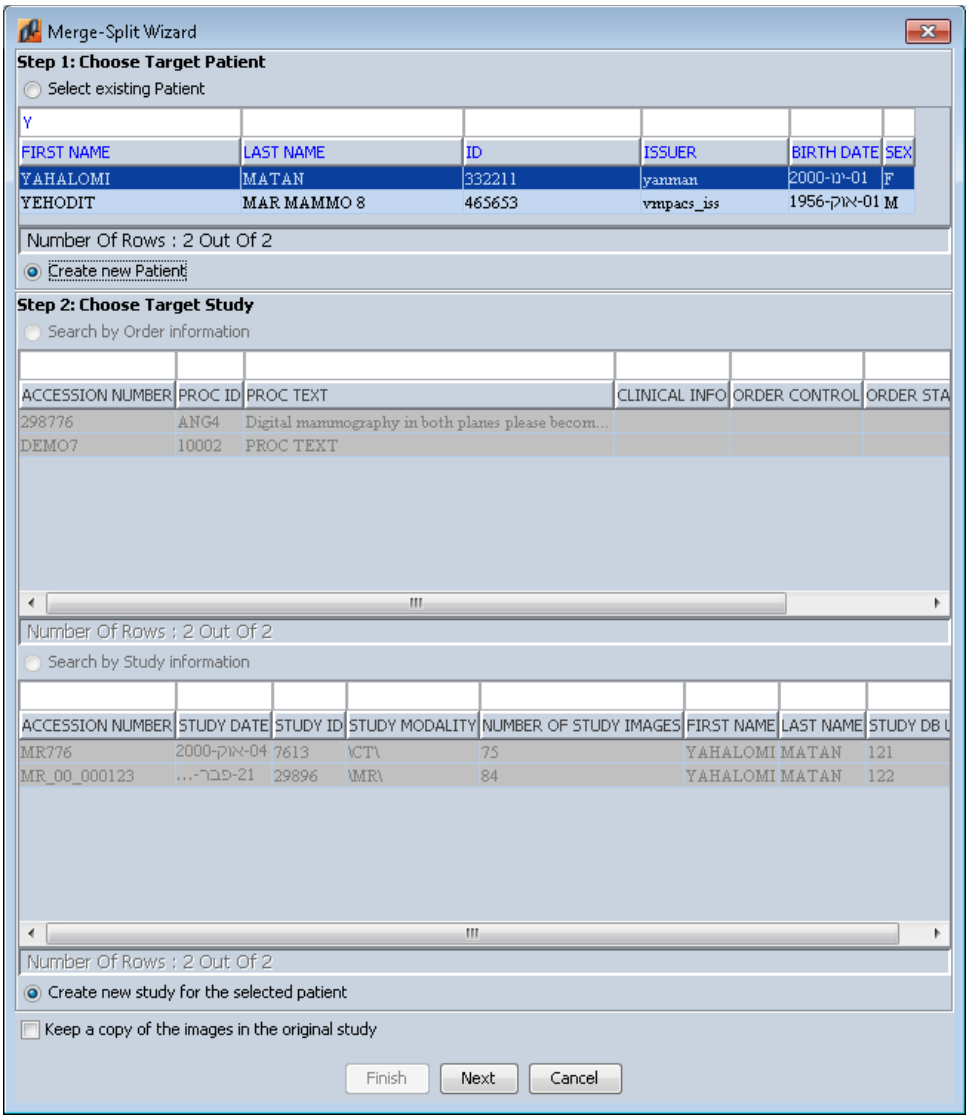
   (You can also select the order and study.)

   The image merges with the selected patient information in the archive.

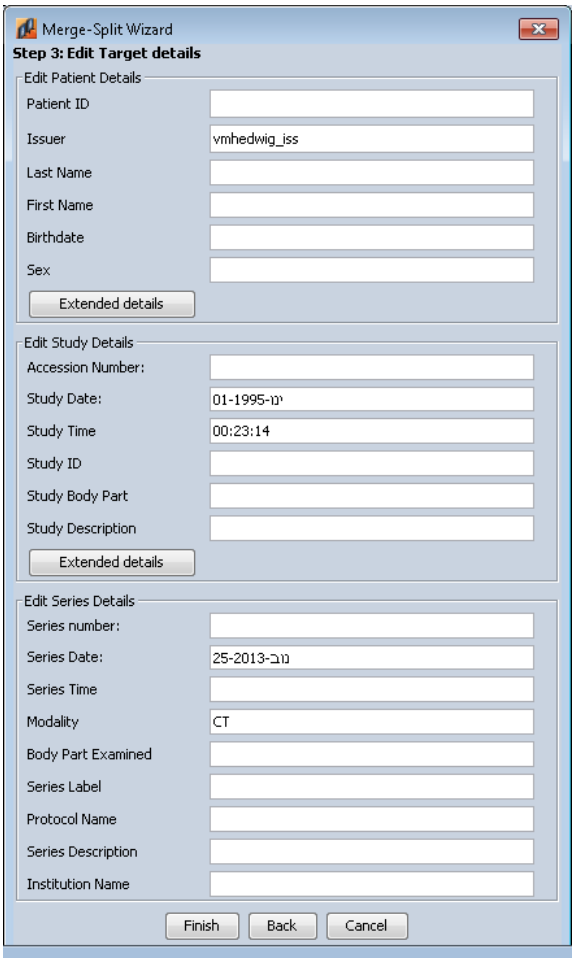
7.1.5.6 Splitting Images

1. In the **Image Details** window, select the images to merge and click **Merge-Split Wizard**  .

   The **Merge-Split Wizard** window appears.



2. Select the **Create new Patient** option and click **Next**.
3. In the **Step 2: Edit Target Study Details** window, complete the new patient data, study, or series data, as required, and click **Finish**.



4. The image is attached to the newly-created patient information, study, or series in the archive.

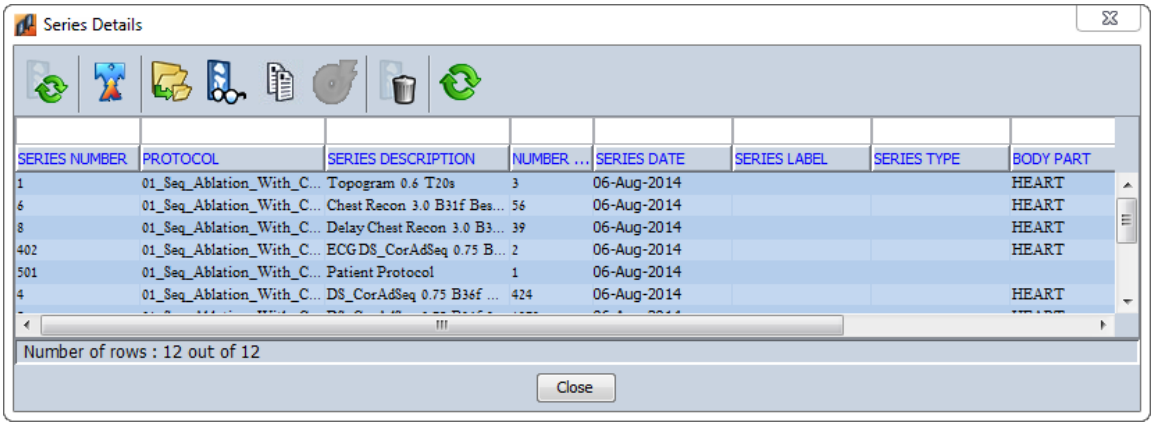
7.1.6 Updating Series Information

You can update information for a series, in addition to the patient and study information.

1. Select the required study in the studies list area.
2. Do one of the following:

   - From the Workflow Manager Administration toolbar, click **Explore Study** 
   - Double-click the study
   - Right-click the required study and select **Explore Study**

   The **Series Details** window appears.



3. Select one or more series to update and click **Update Series**  .
4. If you selected more than one series, click **Yes** in the **Confirm Update** window that appears.
5. In the **Update Series Data** window, update the series as required and click **OK**.

Note: Updating the modality at the series level affects the modality at the study level. If multiple studies are updated at the same time, the **Series Number** field is blocked and changes cannot be made.

7.1.7 Viewing Study Information

You can view images for a selected study. You can also view any report information related to the study being viewed, if available.

1. Select the required study in the studies list area.
2. Do one of the following:
   - Click **View Study** 
   - From the **Edit** menu, select **View Study**
   - Right-click a study and select **View Study**.
3. If the decision of which study to be viewed is not unique (for example, the study does not have an accession number), a window containing all relevant studies appears. Select a study and click **Load** or **Cancel**.

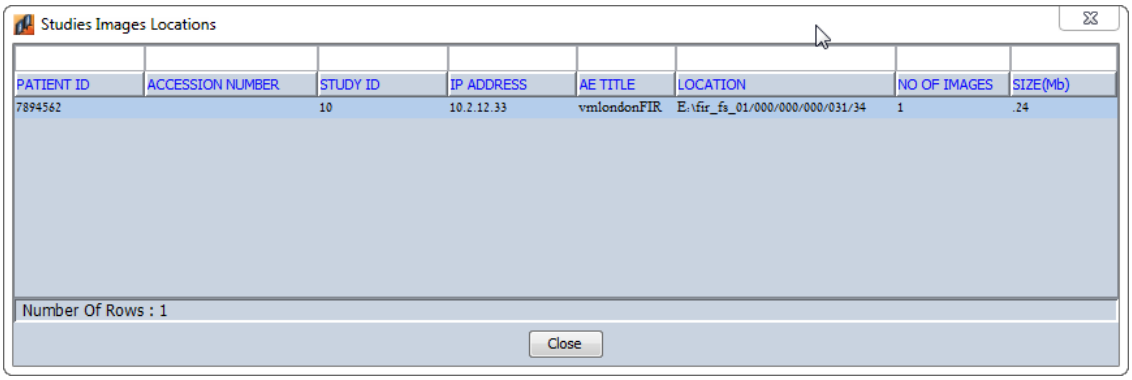
Note: This operation is limited to a single study. If you do not have URL activation permissions, the **View Study** icon is disabled.

7.1.8 Locating Studies

You can search for the locations of an individual study or multiple studies in the system. Each study can reside in multiple locations, as there are always at least two copies of a study in the system at all times.

1. Select a study or studies in the studies list area.
2. Do one of the following:
   - From the Workflow Manager Administration toolbar, click **Study Location** 
   - From the **View** menu, select **Study Location**
   - Right-click the required study and select **Location**

The **Studies Images Locations** window appears, listing the exact location of all copies of the study or studies in the system, as shown in this example:



7.1.9 Viewing Backup Media for Studies

You can view the exact backup media location for near-line studies and offline studies (outside the library).

The Media operation can be performed for an individual study or for multiple studies at the same time. This lets you quickly locate the relevant tape or tapes and determine if they need to be inserted into the Jukebox before you send the Fetch command to the system.

1. Select a study or studies in the studies list area.
2. Do one of the following:

   - From the Workflow Manager Administration toolbar, click **Study Media**  .
   - From the **View** menu, select **Study Media**
   - Right-click the required study and select **Study Media**

   The **Media ID List** window appears.

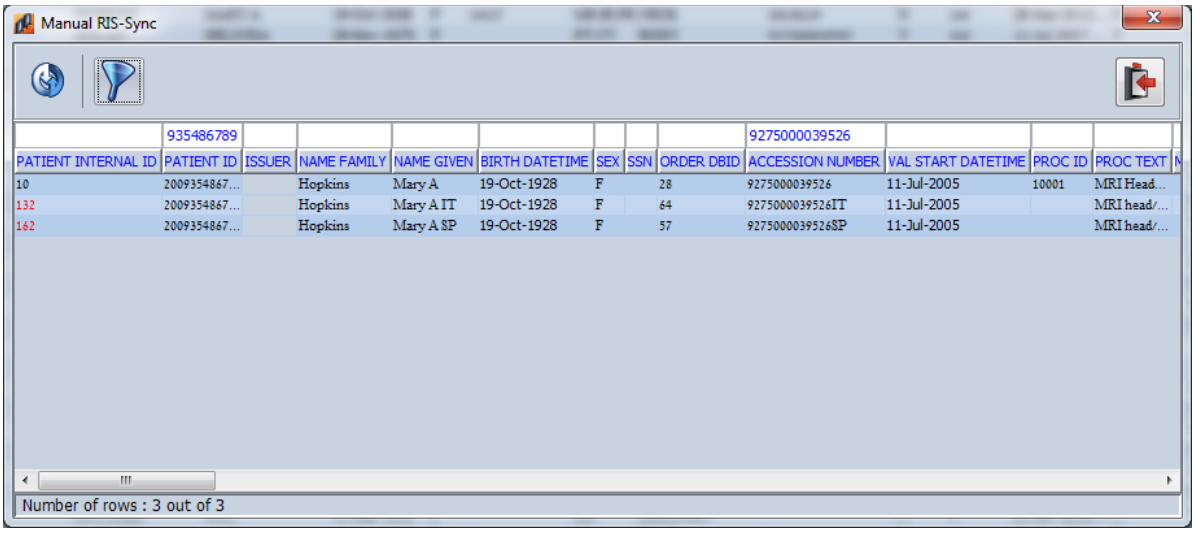
Note: If a study has not yet been backed up on tape, a message appears informing you that the study does not reside on any media.

7.1.10 Performing Manual RIS Synchronization

If the automatic RIS Synchronization process fails for some reason, you can perform RIS synchronization manually. For the manual RIS synchronization to work successfully, both the patient ID and the accession number must be the same.

You can perform manual RIS synchronization on a single study or on a number of studies at the same time.

1. In the Workflow Manager Administration tool, select the study on which to perform the manual RIS synchronization.
2. From the toolbar, click **Manual RIS-Sync**  . The **Manual RIS-Sync** window opens showing details of the orders that relate to the study to be synchronized. The orders are filtered by patient ID and accession number, by default.



3. You can filter the data using more attributes, if required.
4. Select an order and click **Manual RIS-Sync**  .

7.1.11 Protecting and Unprotecting Studies

You can mark one or more studies as protected or change protected studies to unprotected. Studies that are protected are not influenced by the auto-delete process or any manual deletion operation.

To protect a study:

1. Select the required study or studies in the studies list area.
2. From the Workflow Manager Administration toolbar, click **Protect Study**.
3. Click **Refresh**.

   The protection status of the study is displayed in the **Study Locked** column.

To unprotect a study:

1. Select the required study or studies in the studies list area.
2. From the Workflow Manager Administration toolbar, click **Unprotect Study**.
3. Click **Refresh**.

   The protection status of the study is displayed in the **Study Locked** column.

7.2 Working with IS Link

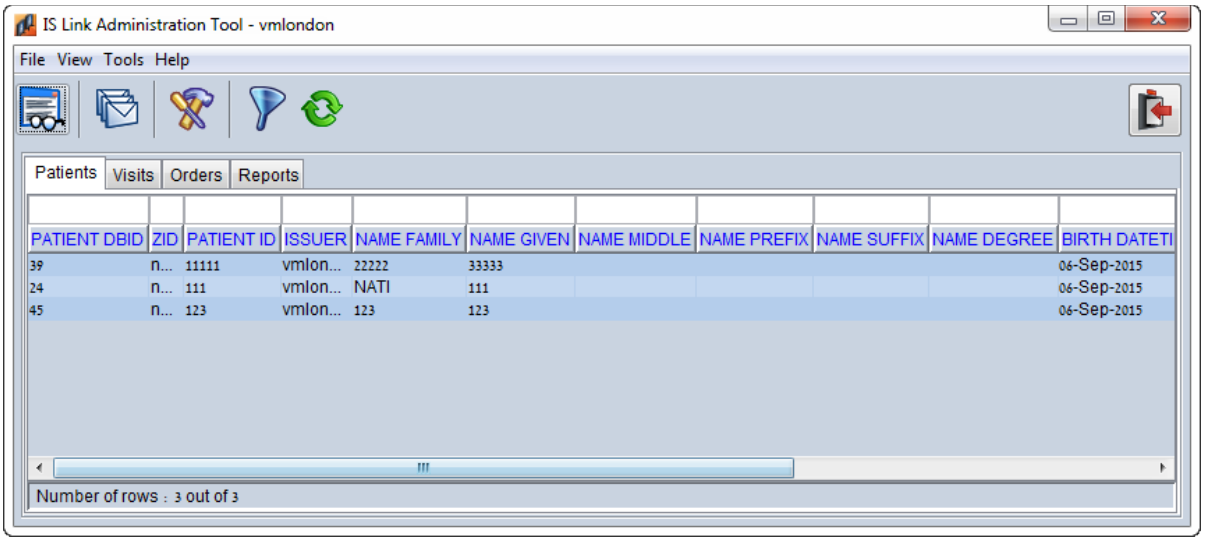
IS Link provides information on patient demographics, visits, and orders, and can be used to retrieve clinical reports.

7.2.1 Getting Started with IS Link

To open the IS Link, select **System Administration > IS Link** from the Administration Tool menu.

In the **Filter** window, enter any relevant parameters to filter the studies shown and click **OK**.

The IS Link Administration Tool opens on the **Patients** tab.



7.2.1.1 Using the IS Link Administration Toolbar

#	Description
1	**View Data—**Click to open the **View Data** window for the selected patient, visit, order or report.
2	**IS Link Queues—**Click to open the **IS Link Queues** window in which you can view the number of notifications for each queue and open the Message queue.
3	**IS Link Central Configuration**— Click to open the **IS Link Configuration Tool** window in which you can change the configuration parameters for the IS Link tool.
4	**Filter**—Click to filter the results shown.
5	**Refresh**—Click to refresh the display with the latest information.
6	**Exit**—Click to close the application.

The IS Link Administration toolbar is page-sensitive; when toolbar functions are not relevant to a particular page, they are grayed out.

7.2.1.2 IS Link Admin Tool Window Tabs

The IS Link Admin Tool window includes the following tabs:

- **Patients** tab
- **Visits** tab
- **Orders** tab
- **Reports** tab

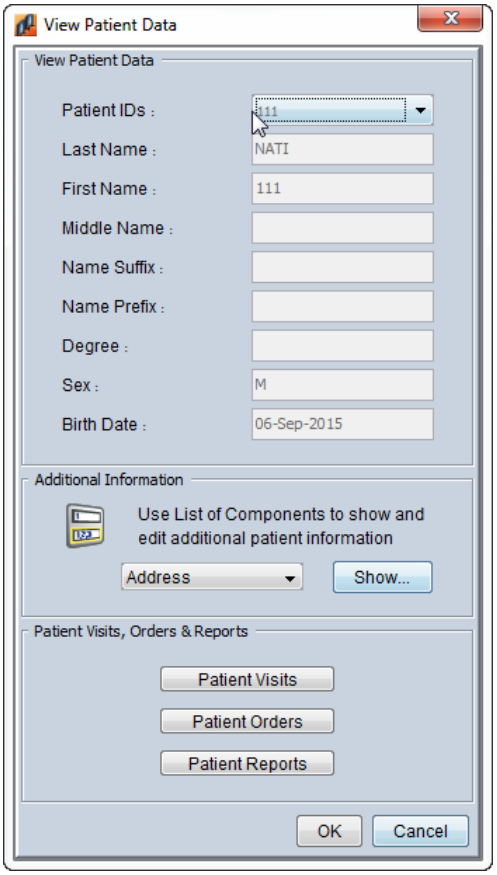
Each tab is related to the previous tab. For example, the **Reports** tab relates to reports that were written based on orders, which in turn refer to particular patient visits. You can search each tab individually using that specific tab, or using the buttons in the **View Patient Data** window.

7.2.1.3 Viewing Patient Information

You can view information for a specific patient in the **View Patient Data** window.

1. In the **Patients** tab, double-click a patient or select a patient and click **View Data** in the toolbar.

   The **View Patient Data** window appears in which you can view patient information.



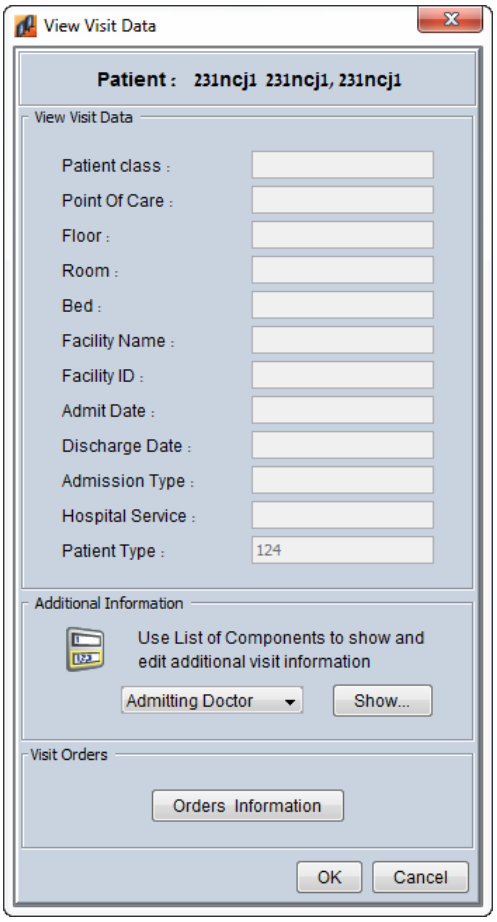
2. In the **Additional Information** section, you can choose to display additional information that is not already displayed.
3. In the **Patient Visits, Orders & Reports** section, you can click the relevant button to view specific visits, orders, and reports of the selected patient.
4. Click **OK** to close the window and return to the **Patients** tab.

7.2.1.4 Viewing Visit Information

You can view information for a specific visit in the **View Visit Data** window.

1. In the **Visits** tab, double-click a visit or select a visit and click **View Data** in the toolbar.

   The **View Visit Data** window appears in which you can view visit information.



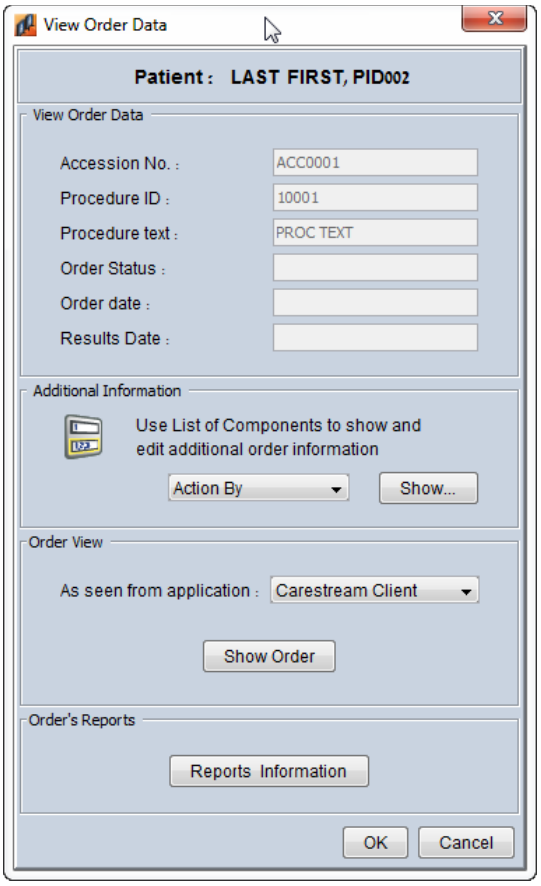
2. In the **Additional Information** section, you can choose to display additional information that is not already displayed.
3. In the **Visit Orders** section, you can click **Orders Information** to view specific orders of the specific patient.
4. Click **OK** to close the window and return to the **Visits** tab.

7.2.1.5 Viewing Order Information

You can view information for a specific order in the **View Order Data** window.

1. In the **Orders** tab, double-click an order or select an order and click **View Data** in the toolbar.

   The **View Order Data** window appears in which you can view order information.



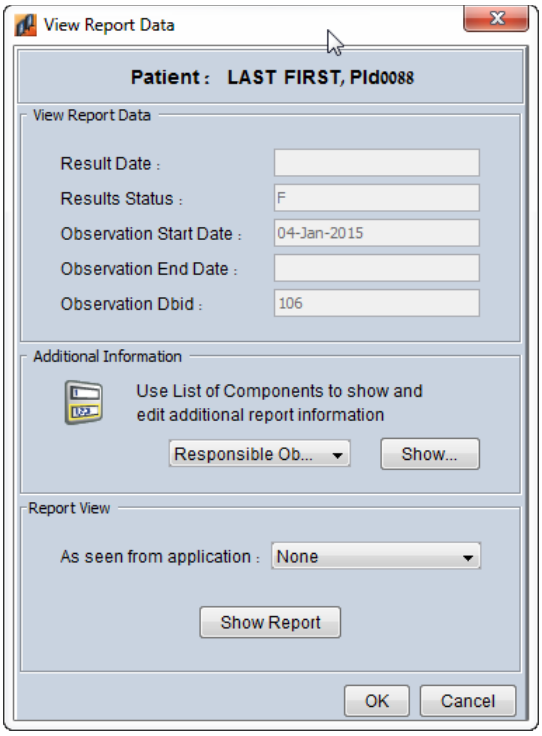
2. In the **Additional Information** section, you can choose to display additional information that is not already displayed.
3. In the **Orders View** section, you can select the relevant application and click **Show Order** to view the order as it appears in the application.
4. In the **Orders Reports** section, you can click **Reports Information** to view reports of the specific patient.
5. Click **OK** to close the window and return to the **Orders** tab.

7.2.1.6 Viewing Report Information

You can view information for a specific report in the **View Report Data** window.

1. In the **Reports** tab, double-click a report or select a report and click View Data  in the toolbar.

   The **View Report Data** window appears in which you can view report information.



2. In the **Additional Information** section, you can choose to display additional information that is not already displayed.
3. In the **Report View** section, you can select the relevant application and click **Show Report** to view the report as it appears in the application.
4. Click **OK** to close the window and return to the **Reports** tab.

7.3 Working with the Certificate Portal

Vue PACS can use secure sockets layer (SSL) to enable secure HTTPS communications between the client Web browser and the Workflow Manager server. Digital certificates are mandatory for SSL connection initialization, and are used to verify that the client workstation is communicating with a trusted server.

Digital certificates are often used when working in a grid environment, where the data center communicates with satellites using secure SSL.

Each site is responsible for obtaining valid certificates from a certified granting authority, or for generating a self-signed certificate. In addition, each site can act as a certificate authority and sign certificates of other sites (for example, in a grid environment).

You can use the Certificate Portal for the following activities:

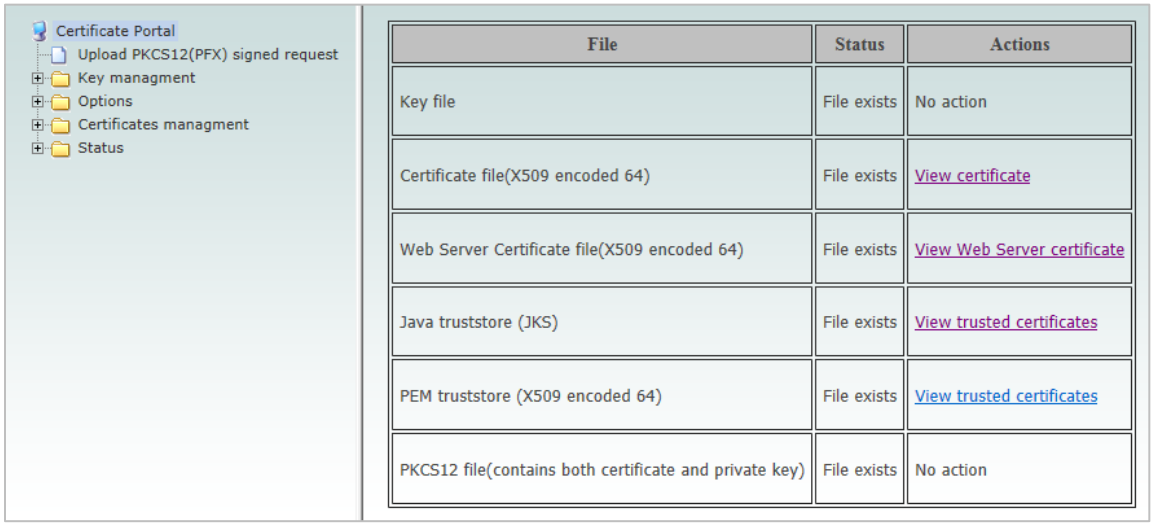
- Managing Keys
- Managing Certificates
- Viewing Certificates
- Testing the Client and Server Configuration

To create a valid certificate and configure SSL in a grid environment, see the example presented in Section 7.3.6 Example: Creating a Valid Certificate and Configuring TLS in a Grid Environment.

7.3.1 Getting Started with the Certificate Portal

To open the Certificate Portal, select **System Administration > Certificate Manager** from the Administration Tool menu.

The Certificate Portal opens showing the links to the various certificate files.

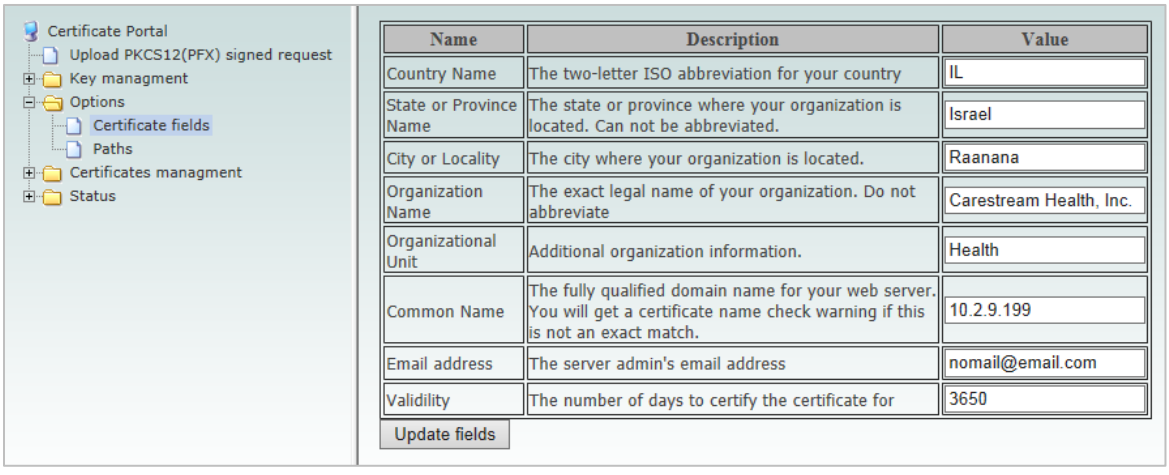


File	Status	Actions
Key file	File exists	No action
Certificate file(X509 encoded 64)	File exists	View certificate
Web Server Certificate file(X509 encoded 64)	File exists	View Web Server certificate
Java truststore (JKS)	File exists	View trusted certificates
PEM truststore (X509 encoded 64)	File exists	View trusted certificates
PKCS12 file(contains both certificate and private key)	File exists	No action

7.3.1.1 Configuring Details for Certificate Requests

You can configure the details that are used to identify your organization in certificate requests. This information only applies to new certificate requests (and will only affect new certificates).

1. In the Certificate Portal, in the left pane, select **Options > Certificate fields**.
2. In the right pane, enter values for the various fields and click **Update fields**.



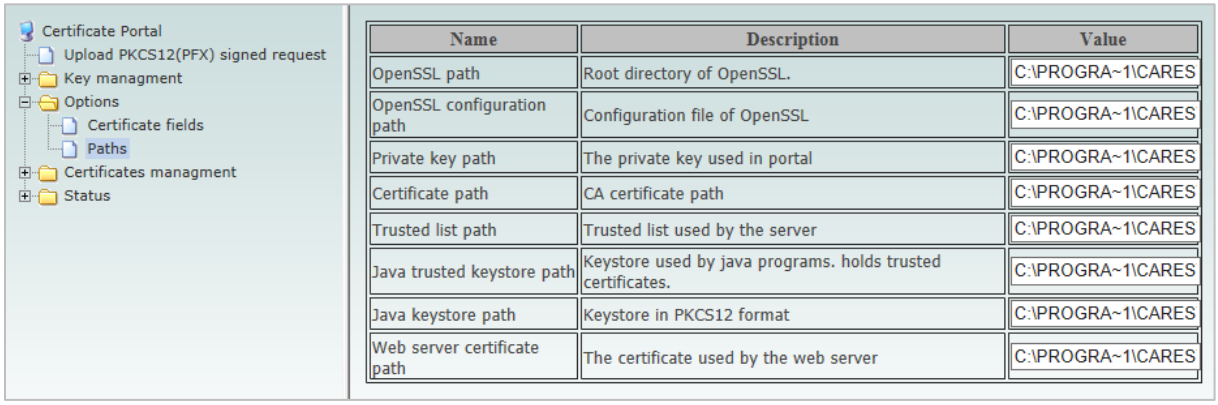
Name	Description	Value
Country Name	The two-letter ISO abbreviation for your country	IL
State or Province Name	The state or province where your organization is located. Can not be abbreviated.	Israel
City or Locality	The city where your organization is located.	Raanana
Organization Name	The exact legal name of your organization. Do not abbreviate	Carestream Health, Inc.
Organizational Unit	Additional organization information.	Health
Common Name	The fully qualified domain name for your web server. You will get a certificate name check warning if this is not an exact match.	10.2.9.199
Email address	The server admin's email address	nomail@email.com
Validility	The number of days to certify the certificate for	3650

Update fields

7.3.1.2 Viewing Certificate File Locations

You can view the locations of various files, such as certificates and trusted lists. The information displayed is read-only and cannot be modified.

In the Certificate Portal, in the left pane, select **Options > Paths**. The following read-only information appears in the right pane.



Name	Description	Value
OpenSSL path	Root directory of OpenSSL.	C:\PROGRA~1\CARES
OpenSSL configuration path	Configuration file of OpenSSL	C:\PROGRA~1\CARES
Private key path	The private key used in portal	C:\PROGRA~1\CARES
Certificate path	CA certificate path	C:\PROGRA~1\CARES
Trusted list path	Trusted list used by the server	C:\PROGRA~1\CARES
Java trusted keystore path	Keystore used by java programs. holds trusted certificates.	C:\PROGRA~1\CARES
Java keystore path	Keystore in PKCS12 format	C:\PROGRA~1\CARES
Web server certificate path	The certificate used by the web server	C:\PROGRA~1\CARES

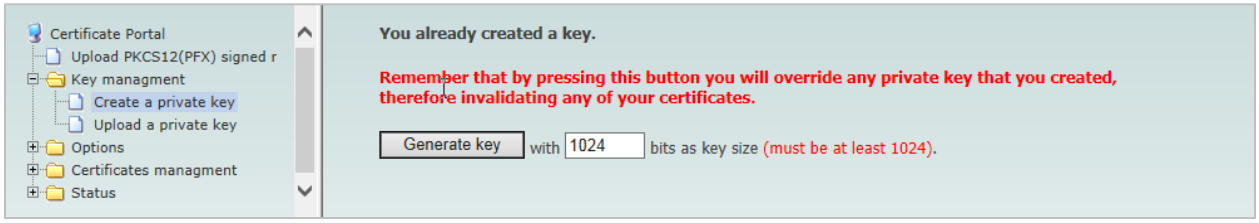
7.3.2 Managing Keys

A default key and certificate is supplied as part of the Workflow Manager installation. You can create and upload a new key to override the existing key; however, this will invalidate any existing certificates and you will need to create a new certificate after this step.

7.3.2.1 Creating a Private Key

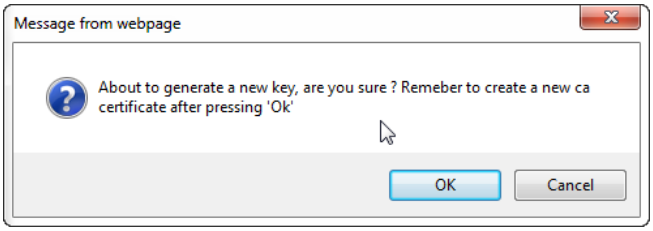
1. In the Certificate Portal, in the left pane, select **Key Management > Create a private key**.
2. In the right pane, enter the number of bits for the key size and click **Generate key**.

   The minimum number of bits is 1024.

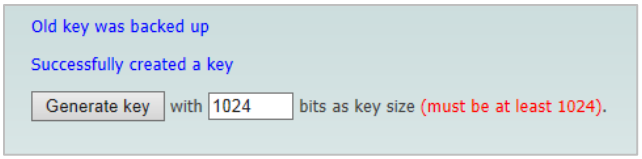


3. In the confirmation message, click **OK** to continue.

   IMPORTANT: This will invalidate any existing certificates. You will need to create a new certificate after this step.



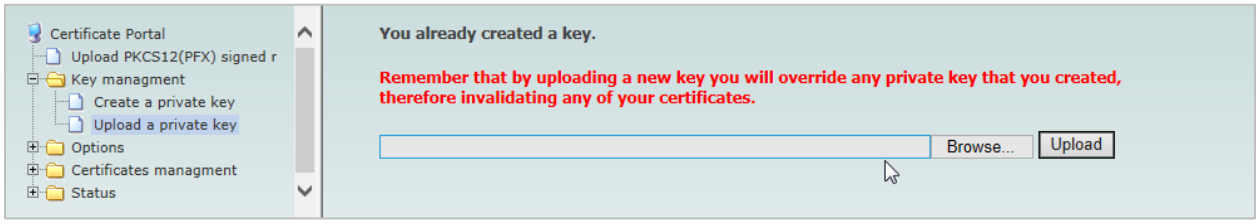
4. Verify that the key is generated successfully.



Now you must create a new certificate. See Section 7.3.3.1 Creating a Certificate Request for details.

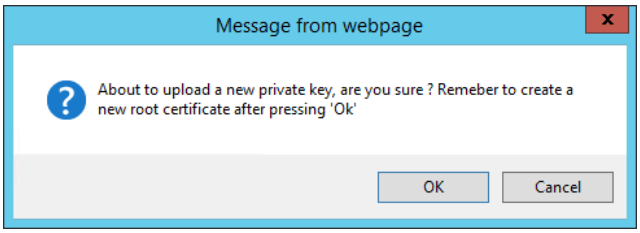
7.3.2.2 Uploading a Private Key

1. In the Certificate Portal, in the left pane, select **Key Management > Upload a private key**.
2. In the right pane, click **Browse** and select the private key file to upload.



3. Click **Upload**.
4. In the confirmation message, click **OK** to continue.

IMPORTANT: This will invalidate any existing certificates. You will need to create a new certificate, or upload the matching certificate, after this step.



5. Verify that the key is uploaded successfully.

Now you must create a new certificate, see Section 7.3.3.1 Creating a Certificate Request, or upload a matching certificate, see Section 7.3.3.3 Uploading a Certificate.

7.3.3 Managing Certificates

A default key and certificate is supplied as part of the Workflow Manager installation. You can create a request to receive a new certificate from a Certificate Authority, and then upload the new certificate to override the existing certificate.

In addition, when working in a grid environment, you can act as a certificate authority and sign certificate requests from satellites in the grid.

Alternatively, you can create a self-signed certificate, which can be used for testing purposes.

7.3.3.1 Creating a Certificate Request

1. In the Certificate Portal, in the left pane, select **Certificates Management > Certificate request**. The certificate request appears in the right pane.

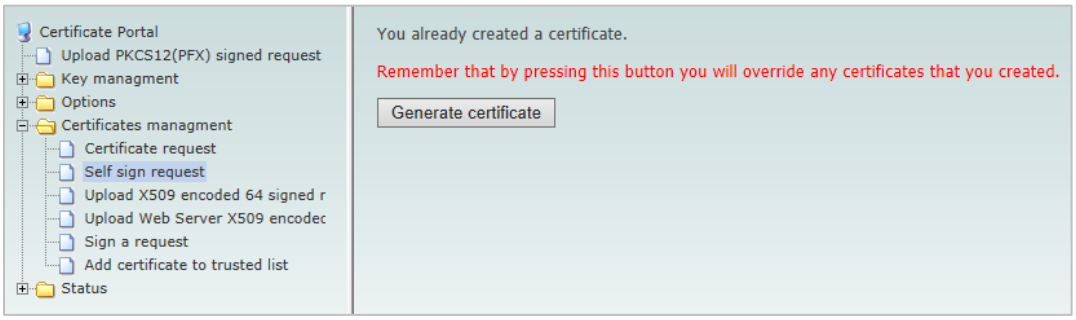
2. Copy the entire text of the certificate request, including the begin and end lines, and save as a text file. For example, `vmnero_cert.txt`.
3. Send the certificate request file to the certificate authority according to your site procedures.

When you receive the signed certificate from the certificate authority, you must upload it to the server. See Section 7.3.3.3 Uploading a Certificate for details.

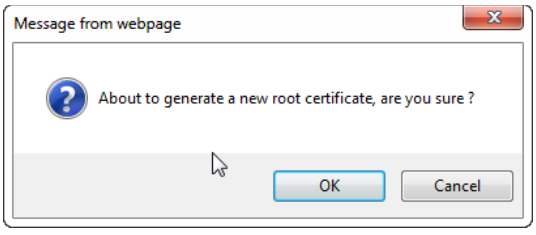
If you want to use a self-signed certificate (for example, if you do not use a certificate authority), you need to create a self-signed certificate. See Section 7.3.3.2 Creating a Self-Signed Certificate for details.

7.3.3.2 Creating a Self-Signed Certificate

1. In the Certificate Portal, in the left pane, select **Certificates Management > Self sign request**.



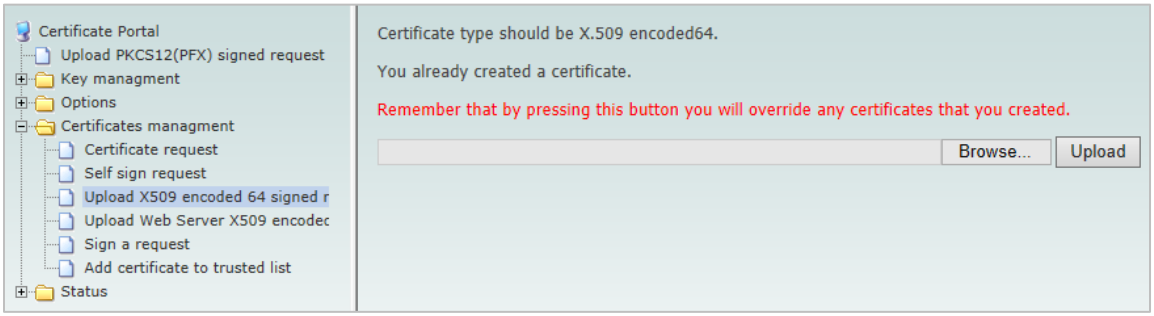
2. In the right pane, click **Generate certificate**.
3. In the confirmation message, click **OK** to continue.



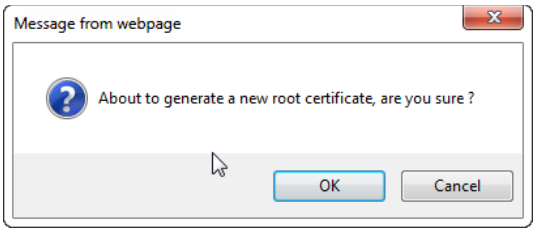
4. Verify that the certificate is generated successfully.

7.3.3.3 Uploading a Certificate

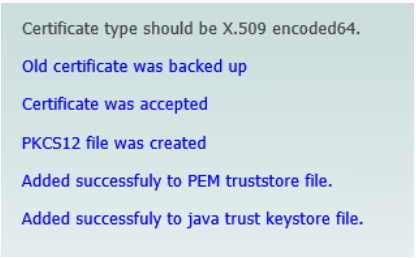
1. In the Certificate Portal, in the left pane, select **Certificates Management > Upload X509 encoded 64 signed request**.
2. In the right pane, click **Browse** and select the certificate file to upload.



3. Click **Upload**.
4. In the confirmation message, click **OK** to continue.



5. Verify that the certificate is uploaded successfully.



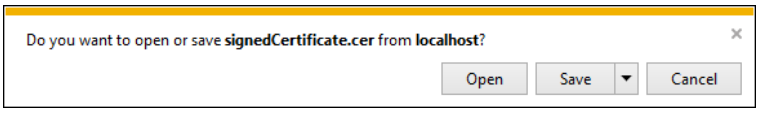
You can also upload an X509 certificate that only applies to the Web server using the **Upload Web Server X509 encoded 64 signed** request option.

7.3.3.4 Signing a Certificate Request

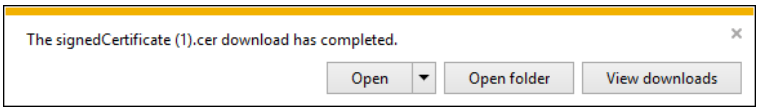
When working in a grid environment, you can act as a certificate authority and sign certificate requests from satellites in the grid.

1. In the Certificate Portal, in the left pane, select **Certificates Management > Sign a request**.
2. In the right pane, browse to the location of the certificate to be signed and click **Upload**.

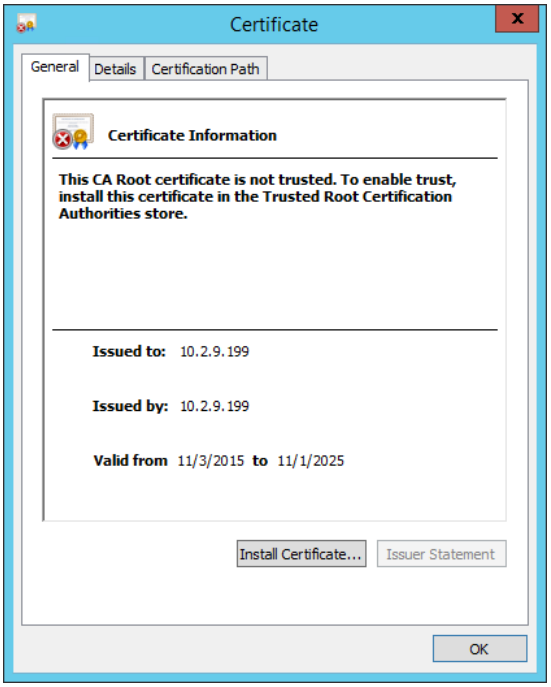
3. In the message that appears, click **Save** to save the signed certificate.



4. To verify that the certificate is valid, click **Open** to open the signed certificate.



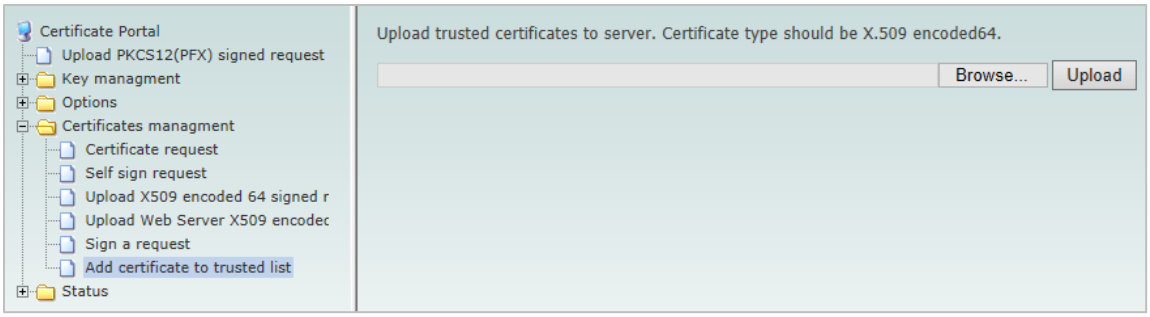
The Certificate window opens showing details of the certificate.



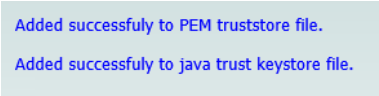
7.3.3.5 Maintaining the Trust List

You can add a certificate to your list of trusted certificates. It is added to both the JAVA-based list (JKS) and the PEM-based list.

1. In the Certificate Portal, in the left pane, select **Certificates Management > Add certificate to trusted list**.
2. In the right pane, click **Browse** and select the certificate file to add to the trusted list.



3. Click **Upload**.
4. Verify that the certificate is uploaded successfully.



7.3.4 Viewing Certificates

You can view current certificates and certificates in the trusted lists. You can choose from the following options:

- Viewing the current root certificate
- View the current Web server certificate
- View the OpenSSL configuration file
- View the Java keystore (JKS) certificates
- View the PEM keystore certificates

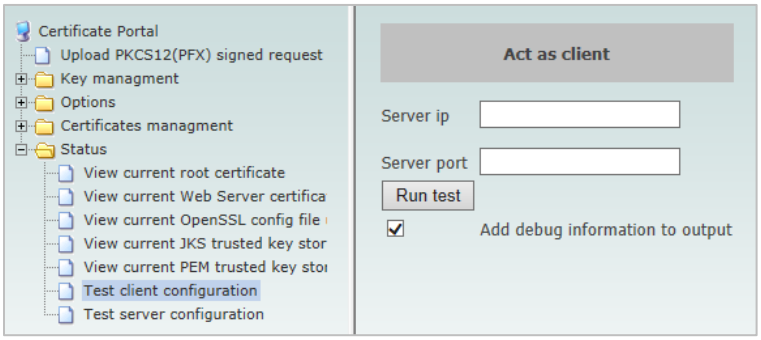
In the left pane of the Certificate Portal, select **Status** and the relevant option.

7.3.5 Testing the Client and Server Configuration

You can test the JAVA client and server configuration. You need to restart APACHE TOMCAT before you perform the testing.

7.3.5.1 Testing the Client Configuration

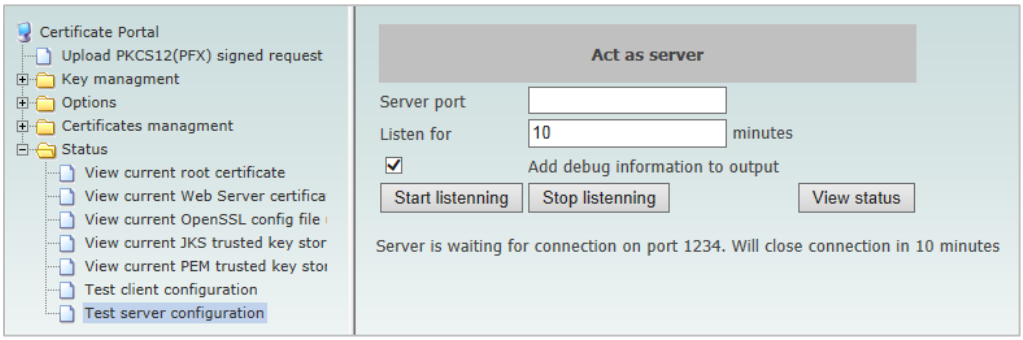
1. In the Certificate Portal, in the left pane, select **Status > Test client configuration**.



2. In the right pane, enter the server IP address and server port and click **Run test**.

7.3.5.2 Testing the Server Configuration

1. In the Certificate Portal, in the left pane, select **Status > Test server configuration**.

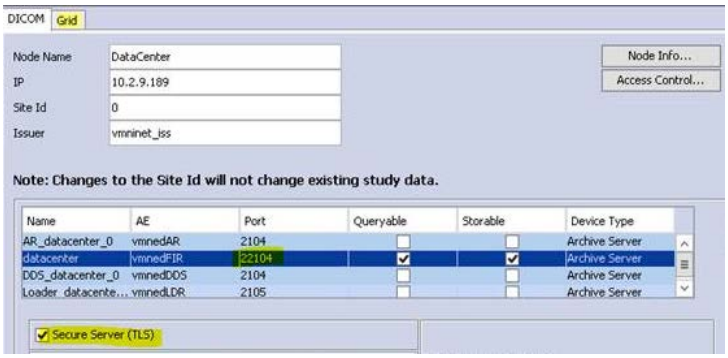


2. In the right pane, enter the server port and amount of time to listen for.
3. Click **Start Listening** and **Stop Listening**, as required.
4. You can view the server status at any time by clicking **View status**.

7.3.6 Example: Creating a Valid Certificate and Configuring TLS in a Grid Environment

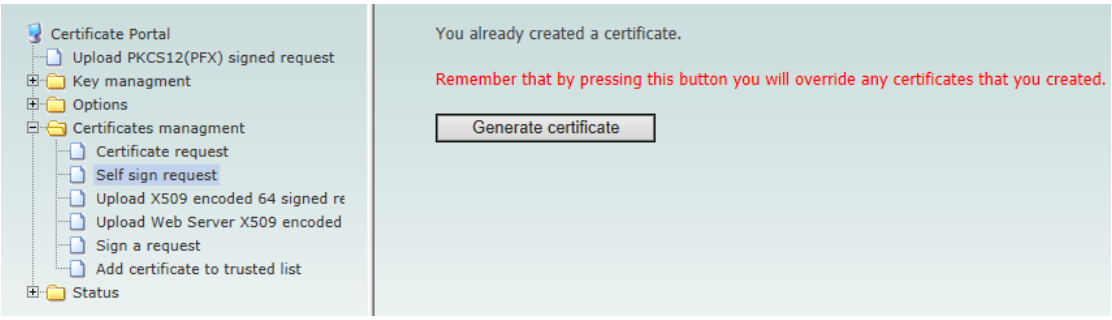
In a grid environment, the data center can communicate with satellites using secure SSL. In this example, you can create a valid certificate and configure TLS in a grid environment.

1. In the System Configuration tool, navigate to **Nodes Configuration** and configure the data center and satellites according to your requirements. Make sure that you define the following settings:
    a. In the FIR port, use 22104.
    b. Select the Secure Server (TLS) check box.



2. Save your changes and close the System Configuration tool.
3. From the data center server, select **System Administration > Certificate Manager** from the Administration Tool menu.

4. In the Certificate Portal, select **Certificates Management > Self sign request**.

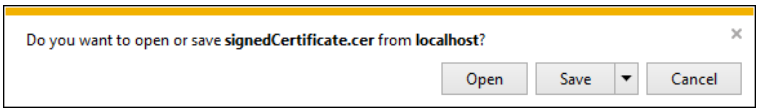


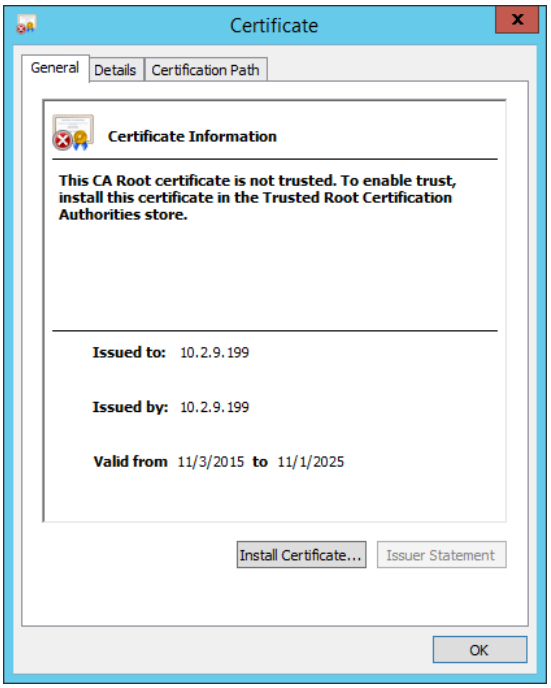
5. Click **Generate certificate**. The new certificate is generated and saved in the default location.
6. To view the new certificate, select **Status > View current root certificate**.
7. Close the Certificate Portal and restart the data center.
8. From the satellite server, select **System Administration > Certificate Manager** from the Administration Tool menu.
9. In the Certificate Portal, select **Certificates Management > Certificate request**.

   The certificate request appears in the right pane.

10. Copy the entire text of the certificate request, including the begin and end lines, and save as a text file. For example, vmnero_cert.txt.
11. From the data center server, open the Certificate Portal.
12. Select **Certificates Management > Sign a request**.
13. In the right pane, browse to the location where you saved the satellite certificate and click **Upload**.

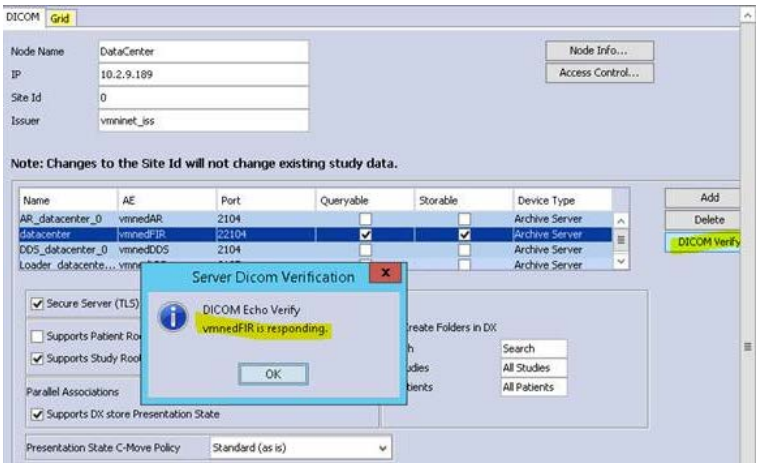
14. Save and open the new certificate.





15. From the satellite server, select **Certificates Management > Upload X509 encoded 64 signed request**.
16. In the right pane, browse to the location where you saved the certificate in the data center and click **Upload.**

17. Close the Certificate Portal.
18. Restart the satellite server.
19. In the System Configuration tool, navigate to **Nodes Configuration** and click the **DICOM Verify** button to ensure that the configuration works correctly.
20. Repeat steps 8-18 for additional satellite servers.



7.4 Working with the Central Configuration Editor

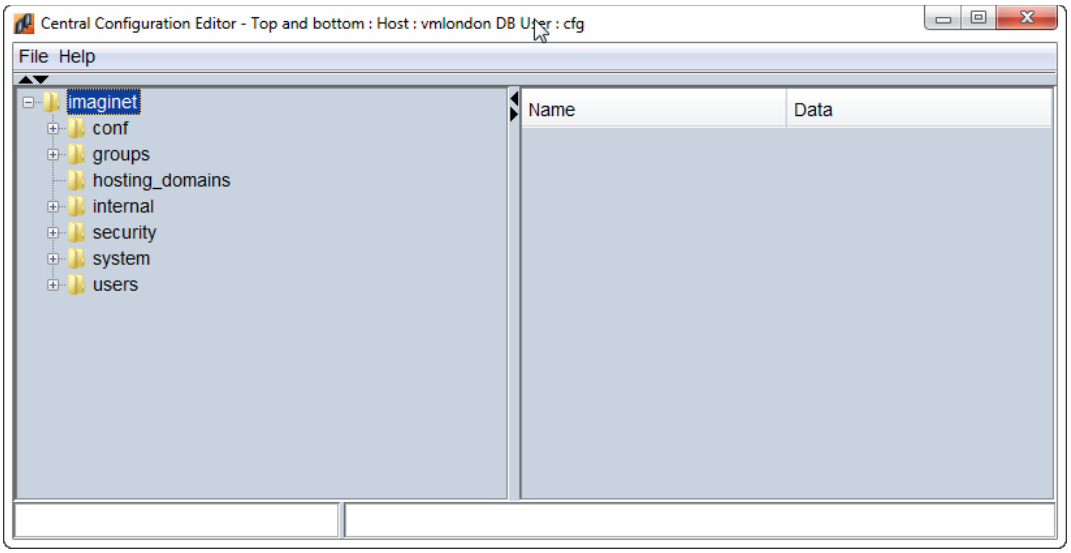
The Central Configuration Editor is a simple repository that enables you to save permanent application information in the Carestream product environment. The Central Configuration Editor is structured as a hierarchical tree, with multiple levels of branches and keys (folders).

IMPORTANT: Exercise caution when changing the Central Configuration. Changing the wrong entries or making an incorrect entry for a setting can introduce an error that prevents the entire system from starting or working properly. Contact Carestream Professional Services personnel for assistance before making any changes.

7.4.1 Getting Started with the Central Configuration Editor

To open the Central Configuration Editor, select **System Administration > Central Configuration** from the Administration Tool menu.

The Central Configuration Editor opens showing the configuration tree in the left pane. You can expand the tree to show all branches, folders, and subfolders. This pane is used to navigate to the required key.



7.4.2 Working with Keys

Right-click the left pane to open a menu with these options:

Option	Description
Add Key	Adds a new key to the tree.
Remove Key	Removes an existing key.
Refresh node	Refreshes the node with the latest information.
Cut	Removes the key from the existing location and saves to the clipboard.
Copy	Copies the key and saves to the clipboard.
Paste	Pastes the key in the target location.
Rename	Renames a key.
Search	Searches for a string under a particular node.
Show Search Result List	Shows the search result list
Search Next	Searches for the next node.
Search Previous	Searches for the previous node.
Go to Path	Navigates to the specified path
Get Entries Count	Counts the number of entries in a particular node.
Import	For advanced users only. Imports data from a file to the Central Configuration repository. The file must be in Carestream format, as created by the Export command.
Export	Exports all the data under the selected key in the hierarchy to a text file. This file is in Carestream format and is compatible for importing.
Dump to XML File	Dumps a subtree in an XML file. The XML format is not compatible for importing.
Copy Path to Clipboard	Copies the selected path to the clipboard.

7.4.3 Modifying Parameter Values

The right pane displays the parameters and values for the selected folder in the configuration editor tree. Use this pane to view specific parameters and values, as well as to modify configurations.

In this pane, parameters can be managed and values assigned to a selected folder. Right-click in this pane to access these options:

Option	Description
Add Value	Adds a new value to the key.
Remove	Removes the selected value from the key.
Copy	Copies the value and saves to the clipboard.
Paste	Pastes the value in the target location.
Cut	Removes the value from the existing location and saves to the clipboard.
Edit Value	Opens the Edit Value window in which you can modify the value.
Select All	Selects all values of the key.
Copy Path to Clipboard	Copies the selected paths to the clipboard.
Copy Path And Value to Clipboard	Copies the selected paths and values to the clipboard.

Appendix A. Maintenance Checklists

Use the checklists provided in this appendix for performing daily, weekly, and monthly tasks.

A1. Daily Maintenance Tasks

Perform the following tasks on a daily basis:

Task	Procedure	Comments
Check that Info Router commands are processing	1. Log in to **Administration Tool > System Monitoring > Info Router** to open the Info Router client. 2. Check for failed/waiting commands and retry commands to get them to succeeded state. 3. Check for backlog in Not Started queues. 4. Verify Info Router activity and make sure that commands are running and transitioning to succeeded state. 5. Stop and start Imaginet Auto-Router Server service if needed (log in to Administration Tool > System Monitoring > Server Processes) See Section 5.2 Using the Info Router for more information.	Make sure that the Info Router is working. If there is a problem and commands are not going to succeeded state, contact Customer Service.
Run a system check	1. Log in to **Administration Tool > System Monitoring > System Check**. 2. Select the relevant local node and click **Run System Check**. 3. Review the warning and critical error messages. The most important categories to monitor include: • Uptime • Storage partition filling • General system partition filling • Remote DICOM Connectivity • Studies Need Backup • Oracle Status • Oracle Backup • CFG Backups Note: Other categories are also important but do not affect maintenance as much. See Section 5.1.3 Running System Checks for more information.	If you have a critical error, which cannot be explained, contact Customer Service.

Task	Procedure	Comments
Check Oracle database backup	1. In WINDOWS, select **Start > Administrative Tools > Task Scheduler**. 2. Select the relevant scheduled task and check that the date in the **Last Run Time** column is today's date. The following scheduled tasks are defined: • run_al_backups • run_cold_backups • run_full_backups 3. Navigate to `<Backup_drive>:\oradata\mst1\backup` and check whether the name of the log file includes the status `ok` or `err`. See Section 6.3 Verifying the Database Backup for more information.	A daily task runs at 6 am to ensure that the previous backup was successful. You can also perform this backup verification manually when there is a related problem reported by the system check. If there is a problem, contact Customer Service.
Check Central Configuration backup	Make sure that the Central Configuration backup completed successfully. You can do this from the System Check or by manually checking the `(servername)_cfg.exp.1.log` (look at the end of the file to verify that the export terminated successfully without warnings). See Section 6.5 Backing up the Central Configuration for more information.	If there is a problem, contact Customer Service.
Check if any studies need backing up	Check whether any studies need backing up. You can do this from the System Check or by filtering by Study Need Backup = Y in the Workflow Manager Administration tool. You can also check whether the **Needs Backups** Info Router commands are succeeding.	Contact Customer Service if the count of studies older than 48 hours is growing, or if there is problem archiving data to the backup device.
Check partition filling (Storage and General System)	Check the Storage and General System partition filling amounts. You can do this from the System Check or by manually checking the total size and available free space of partitions in Windows Explorer. You can also review the Storage Partition filling in **Administrator Tool > System Configuration > Application Configuration > Life Cycle Management > Archive Configuration**.	Contact Customer Service if free space is above defined high watermark thresholds for Storage partition filling or is indicating a critical error in the System Check. Approximately 20% minimum free space is recommended but this can vary depending on the system and overall storage size.

Task	Procedure	Comments
Check services are running	Check whether services are running by logging in to **Administration Tool > System Monitoring > Server Processes** or in WINDOWS from **Start > Administrative Tools > Services**. Check that the following services are running: AppFabric Event Collection Service AppFabric Workflow Management Service IIS Admin Service APACHE TOMCAT FLEXlm Service Imaginet Auto-Router Imaginet CDDirect Server Imaginet DB Audit Imaginet Failover Imaginet Loader Imaginet MediLink Converter Imaginet MediLink Listener Imaginet Medilink Sync Listener (only if synchronization is configured) Imaginet MstSync Server (only at data center if synchronization is configured) Imaginet MVSMain Secured Imaginet MVSMain Server Imaginet RisSync Server Imaginet Startup-Shutdown Imaginet System Check Imaginet Task Dispatcher Imaginet Task Scanner Imaginet WCF Mirth OracleOraDB12Home1TNSListener OracleServicemst1 Redis See Section 5.1.4 Monitoring Server Processes for more information.	Attempt to start/restart a service that should be running and not disabled. Contact Customer Service if service cannot be started/restarted
Check scheduled tasks	From the WINDOWS Task Scheduler, check that all tasks ran and completed successfully (including fir_autodelete, Db Worker, and backups). See Section 6.8 Running Other Scheduled Database Maintenance Tasks for more information.	Contact Customer Service if an enabled task is not completing successfully.
Check IS Link queues	Check for backlogged queues via **Administration Tool > System Administration > IS Link Administration Tool >>IS Link Queues**. The number of notifications should be zero or working its way down to zero.	Attempt to start/restart the Imaginet Medilink Converter Service to see if the queues start to process down. If queues are growing, contact Customer Service.

Task	Procedure	Comments
Check study statuses are up to date	You validate study statuses by reviewing data in the Vue PACS Client or from Workflow Manager Administration filtered queries. Make sure that the studies are in expected statuses. For Vue Reporting, ensure studies are not stuck in **Pending** or **Processing XXX** statuses.	Depending on the defined workflow, status changes should be happening automatically. If not, contact Customer Service.
Check RIS Synchronization status of studies	Search for $$$ in the Patient ID column. In the Workflow Manager Administration tool, query for %$%. Merge patients into correct patient data, then perform a RIS synchronization. In the RIS Synch column, query for `N`. In RIS, investigate if there is an order or problem with the study, then perform the RIS synchronization.	
Check the Synchronization Monitor (only relevant for Vue Connect sites or sites with Downtime Backup server)	Check for metadata synchronization issues via **Administration Tool > System Monitoring > Synchronization Monitor**. Verify that the last communication time for the remote site is as close to the current time as possible. Verify that the Sync Gap is not indicating a warning or error.	Contact Customer Service if the last communication time is not current or the Sync Gap is widening.
Monitor VERITAS cluster status (only relevant for cluster environments)	Log in to the VERITAS Cluster Explorer via the VERITAS Cluster Manager and verify that all resource groups are online and running. Verify that the resource groups are running on the expected node.	Contact Customer Service if resource groups are not fully online, or if the resource group is running on a different node than expected.
Check the ORACLE alert file	The ORACLE database has a built-in alert file, in which system alerts and important messages are registered. You should read this file daily to identify potential problems at an early stage, as follows: 1. Navigate to: `<DB_drive>:\imaginet_db\oracle\admin\diag\rdbms\mst1\mst1\trace\alert_mst1.log` 2. Open the alert file using Notepad or WordPad. 3. Scroll down to the last section of the file. 4. Locate the last week's dates and review the messages. 5. Only informative messages are acceptable, such as startup, shutdown, and changing log files. (Thread 1 advanced to log sequence) See Section 6.6 Checking the ORACLE Alert File for more information.	Contact Customer Service if an error exists.

A2. Weekly Maintenance Tasks

Perform the following tasks on a weekly basis:

Task	Procedure	Comments
Check load balancers (if in use)	Ensure that both load balancers in front of the Downtime Backup server or Vue Motion servers are operational.	Contact Customer Service if a load balancer is not operational.
Check server room hardware	Verify if there are amber lights on the following: • Production server • Downtime Backup server • RAID • Archive server • RIS server • Tape Library Check the status of UPS units or back up power sources.	Contact vendor support or Customer Service, as appropriate.
Reboot the reading workstations	Restart the reading workstations: **Start → Shutdown → Restart**	
Check the ConText adaptation on the Speech Server (for Vue Reporting sites only)	1. Go to **Start > Programs > SpeechMagic > ConText Adaptation**. 2. Select the ConText to review and click **OK**. **Note:** There should only be one ConText available for review. 3. Go to the **Handle Unknown Words** tab to address any unknown words, adding all that are relevant. **Note:** Only select **Add** or **Ignore Now** when managing unknown words. Do not to use **Ignore Always** to do a mass cleanup of unknown words. Only use this button when there are reoccurring instances of individual illegitimate words. See *CARESTREAM Vue Reporting 12.1 Administration Guide* for more information.	
Confirm SPEECHMAGIC services are running or active on the Speech Server (for Vue Reporting sites only)	1. To access the Service Viewer, go to **Start > Programs > SpeechMagic > Tools> Service Viewer**. 2. Validate that `NT Service` is Running, and `RcgTask`, `PurgeTask`, and `CtxtTask` are Active. 3. If not running, right- click and select **Stop SpeechMagic Windows Service**, and then **Start SpeechMagic Windows Service**.	Contact Customer Service if service or tasks will not go to running or active states.

A3. Monthly Maintenance Tasks

Perform the following tasks on a monthly basis:

Task	Procedure	Comments
Install MICROSOFT WINDOWS updates	Install MICROSOFT WINDOWS Security and Critical updates. Do this before rebooting the server.	
Reboot servers	Reboot all servers.	
Validate Downtime Backup server functionality	Verify workflow by testing complete workflow (book one exam, check the HL7 message arrives in PACS, and the worklist on the modality, acquire one exam, send it to PACS, check RIS-PACS synchronization, check reports arrive in PACS). You can also transition complete site to Downtime Backup server prior to performing monthly WINDOWS updates and server reboot on production server.	

A4. Situational Maintenance Tasks

Perform the following tasks when required:

Task	Procedure	Comments
Test the workflow	Test the complete workflow: 1. Book one test exam. 2. Check the HL7 message arrives in PACS from IS Link. 3. Check the HL7 message arrives in the DICOM Modality Worklist query on the modality. 4. Acquire images for the test exam. 5. Send the test images to PACS. 6. Verify RIS-PACS synchronization. 7. Dictate/mark the test study as READ/FINAL. 8. Check reports arrive in PACS/RIS.	

Task	Procedure	Comments

Shut down and restart PACS services	If you need to restart PACS application services, do the following:
	• To stop PACS application services, open a command prompt as administrator and type:
	`system5_shutapp`
	• To restart PACS application services after the services have been shut down, enter the following command:
	`system5_startapp`
	If you need to restart PACS application services as well as the database services, do the following:
	• To stop PACS application services and database services, open a command prompt as Administrator and type:
	`system5_shutdown`
	• To restart PACS application services and database services after all services have been shut down, enter the following command:
	`system5_startall`
	or perform a WINDOWS reboot to the server and everything will start up following the reboot.	

Monitor the calibration	Make sure the calibration is current and good for the diagnostic monitors. Follow best practices determined by state guidelines or a medical physicist.	
Monitor the bandwidth	Log in **to Administration Tool > System Monitoring > Bandwidth Test** and do the following: • Test the bandwidth between your workstation and the local node • Test the bandwidth between the local node and remote nodes • Test the bandwidth between server nodes using the command line See Section 5.1.7 Monitoring the Bandwidth for more information.	Test the bandwidth when directed by Customer Service. Check periodically to establish expected baselines.

Task	Procedure	Comments
Perform an ORACLE server general fitness check 12.1 Admin Guide Section 6.7	When the system is restarted, or after a failure or invoked operation, such as installation, upgrade or restructuring, you must ensure that all of system components are functioning properly. You should perform the ORACLE Server general fitness check manually after every reboot. When the system is up, these services should be running: • OracleServicemst1 – The Workflow Manager database service • OracleOraDB12Home1TNSListener – The ORACLE Listener service See Section 6.7 Performing an ORACLE Server General Fitness Check for more information.	Contact Customer Service if there is a problem.

CARESTREAM is a trademark of Carestream Health.

© Carestream Health, Inc. 2015

Carestream Health
150 Verona Street
Rochester, NY 14608
United States

Made in the USA

Pub No. 9J8767 v2.0